Rapid Technology Application Program

Broad Agency Announcement 05-10

(BAA 05-10)

Department of Homeland Security

Homeland Security Advanced Research Projects Agency (HSARPA)

November 28, 2005

Mandatory White Papers Due: 3 January 2006

Proposals Due: 6 March 2006

For Questions Regarding This Solicitation:

BAA05-10@dhs.gov

FINAL

TABLE OF CONTENTS

FINAL

FINAL

1 BACKGROUND

The Science and Technology (S&T) Directorate in the Department of Homeland Security (DHS) has the mission to conduct research, development, test and evaluation (RDT&E) and timely transition of homeland security capabilities to operational units within DHS, as well as Federal, State, local and critical infrastructure sector operational end users for homeland security purposes.

The Homeland Security Advanced Research Projects Agency (HSARPA) invests in programs offering the potential for revolutionary changes in technologies that promote homeland security and accelerates the prototyping and deployment of technologies that reduce homeland vulnerabilities. HSARPA is the external funding arm for the DHS S&T. HSARPA performs these functions in part by awarding procurement contracts, grants, cooperative agreements, or other transactions for research or prototypes to public or private entities, businesses, federally-funded research and development centers and universities.

2 PROGRAM OBJECTIVES AND APPROACH

HSARPA is initiating the Rapid Technology Application Program (RTAP) to meet the expressed rapid technology development needs of emergency responders and internal DHS customers. The RTAP will facilitate a number of HSARPA's goals, including:

- Fulfilling the expressed needs of emergency responders and internal DHS customers for rapid prototype technology developments
- Producing advanced technology prototypes 6-18 months after award of contracts

In this solicitation HSARPA is soliciting white papers and proposals for the rapid prototyping of systems in the following seven specific technical fields: Explosive Countermeasures, Biological Countermeasures, Chemical Countermeasures, Information Technology – Geospatial, Information Technology – Information Sharing, Electronics and Hardware, and Cyber Security. The 22 Topics identified for these specific technical fields are listed below.

Explosive Countermeasures (EC) Topics:

- EC1 - Maritime Safety and Security Team (MSST) Explosive Trace Detection
- EC2 - Non-invasive Portable Object Examination System
- EC3 - Advanced Capability X-ray System for Bomb Squad

Biological Countermeasures (BC) Topics:

- BC1 - Rapid Suspected Bio-agent Screening
- BC2 - Aircraft "Spot" Decontamination
- BC3 - Biosurveillance Detection Algorithms
- BC4 - Rapid Field Identification of High Priority Plant Pathogens (RFIP)

FINAL

Chemical Countermeasures (CC) Topics:

- CC1 - NIOSH CBRN 60 Tactical Escape Mask
- CC2 - Escape Hood

Information Technology – Geospatial (ITG) Topics:

- ITG1 - Transportation Route Risk Analysis and Resource Allocation Tool
- ITG2 - Significant Encounters Visual Environment (SIEVE)
- ITG3 - Modeling the Complex Urban Environment (MCUE)

Information Technology – Sharing (ITS) Topics:

- ITS1 - Geospatial Modeling of Homeland Security Capabilities
- ITS2 - Resource Awareness Data Portal
- ITS3 - Tactical Information Sharing System (TISS) Image Analysis Capability

Electronics and Hardware (EH) Topics:

- EH1 - Advanced 3-D Locator System
- EH2 - Extreme Wide Field-of-View IR/NV Capability
- EH3 - Improved Heartbeat Detector System Prototype
- EH4 - Advanced Urban Search and Rescue (US&R) Breaching Approach

Cyber Security (CS) Topics:

- CS1 - BOTNET
- CS2 - Exercise Scenario Modeling Tool
- CS3 - DHS Secure Wireless Access Prototype

To achieve the program goals, this Broad Agency Announcement (BAA) calls for rapid development of technologies in the 22 Topics listed above. Offerors are invited to prepare proposals to address one or more of the 22 Topics described in greater detail in Section 3, but should submit a separate proposal for each topic addressing only one proposed approach or concept per topic. Further details on multiple submissions are provided in Section 5.

2.1 Program Structure

RTAP will develop and field test selected prototypes within 6-18 months after contract award. The successfully tested prototypes will be part of the final deliverables for this base effort.

RTAP awards will consist of a base period not to exceed 18 months. In addition, offerors may propose an option not to exceed 12 months if appropriate for that topic. The offeror should carefully read and respond to the specific topic. The failure to propose a requested option will lower the evaluation under evaluation criterion 1.

Base period requirements - Offerors are required to produce a working prototype based upon the requirements outlined in the BAA. The base period is not to exceed 18 months. Offerors should indicate if the prototype can be field tested during this period. If so, costs for field testing should also be included in this base period. The total funding requested from HSARPA may not exceed

FINAL

$2 Million (M) for the base effort. **Any proposal where the base effort exceeds $2M will be considered non-responsive.**

Option period requirements – Offerors may propose additional research and development or field testing of the prototype model beyond the base year to satisfy the option specified in the appropriate topic. The government reserves the right not to accept this option and/or not to exercise this option. The government also reserves the right to compete an option for additional research and development, field testing or limited pre-production quantities of the prototype. If more than one option period is requested within a topic, offeror should price each option separately. In no event may the period for an option exceed 12 months nor any combination of options exceed 12 months. However, multiple options may run concurrently.

2.2 Government Furnished Equipment, Resources and Information (GFE, GFR, GFI)

The government will provide GFE, GFR, and/or GFI under the terms of each specific topic. The provided GFE, GFR, and/or GFI do not have to be factored into the project cost. However, GFE, GFR, and/or GFI requested by an offeror, which will not automatically be provided by the government under the terms of the topic, must be factored into the offeror's project cost. Combined direct funding and GFE, GFR, and/or GFI may not exceed $2M for the base effort of the proposal. **Any proposal where the base effort exceeds $2M will be considered non-responsive.**

2.3 Hazardous Materials

Depending on the topic, offeror may choose to or be required to utilize hazardous materials during the course of the project development effort. If the government provides hazardous samples as part of the developmental and operational testing, information on the samples will be provided to the successful offerors requiring such samples. Hazardous material, as used here, includes any material defined as hazardous under the latest version of Federal Standard No. 313 (including revisions adopted during the term of the contract). If the successful offerors choose to use their own hazardous samples, offerors must meet the requirements for the identification and material safety in Appendix D.

2.4 Request for Government-Only Review

Government and non-Government experts who have signed appropriate non-disclosure agreements will support the HSARPA Program Manager in performing technical evaluation of white paper and proposal submissions. Offerors who wish to have their white paper or proposal reviewed exclusively by Government personnel must indicate so during the mandatory white paper registration. If the cover page is not properly marked for Government review only due to the failure to properly request Government-only review at the time of white paper registration, then the Government shall not be liable for inadvertent release of any white paper or proposal information to non-Government reviewers. Notwithstanding a request for a Government-only review, the Government will use contractors to administratively handle the submissions. These personnel will have signed, and will be subject to, the terms and conditions of non-disclosure agreements.

FINAL

2.5 Test and Evaluation Facilities

Department of Homeland Security Science & Technology Directorate may make available appropriate test and evaluation facilities to support this program. Offerors should provide any specific requirements needed for test and evaluation of their proposed concept in their mandatory white papers and proposals.

3 PROTOTYPE PERFORMANCE GOALS

The performance targets, cost of ownership, and prototype characteristic goals the Government seeks to achieve are very ambitious.

For a white paper or proposal to be considered responsive, the proposed prototype must meet all required goals and meet as many of the desired goals listed in the topic description as possible.

3.1 RTAP Topics

Rapid prototyping projects have been generated by a full range of DHS operational entities for their most urgent needs. These users have identified their highest priority projects for rapid prototypes as topic areas, which encompass seven technical fields. The 22 Topics are detailed below, each of them describing the requirements of the solicited rapid prototype. Offerors must submit only one topic per mandatory white paper and proposal and must address only one proposed approach or concept per topic.

3.1.1 Explosive Countermeasures (EC) Topics:

3.1.1.1 EC1- Maritime Safety and Security Team (MSST) Explosive Trace Detection

Descriptive Title:

Maritime Safety and Security Team (MSST) Explosive Trace Detection

Current trace detection capabilities exist [Ion Mobility Spectroscopy (IMS), canine, etc.]; however, these capabilities need to be improved for operation in complex maritime/industrial environments. A key operational consideration is that the explosive trace detection missions performed by MSSTs (surveying of a vessel or shore side facility) require a wide-area search and are therefore not conducive to a checkpoint scenario. While it is anticipated that the time/resources available to conduct Explosive Trace Detection (ETD) operations will be dependent on vessel/facility size, a key, overriding requirement is not to unduly delay maritime commerce. Therefore, the Department of Homeland Security (DHS) needs a small, rugged, portable device which is capable of accomplishing explosive trace detection onboard assorted vessels and facilities in maritime environments, which are often complicated by various interferants (e.g., diesel fuel, saltwater spray, cargo substances, chemical).

Description & Specifications:

The contractor shall develop a prototype demonstrating improved capabilities for explosive trace detection in the maritime environment. The contractor shall use an iterative development and testing approach, working closely with the government. The contractor shall include in the

proposal two options[1]: one for additional testing prototypes in lots of 50 or more, and a second for operational support of prototype units in the field. During this project, the contractor shall develop a prototype to meet the following characteristics:

Note: Proposals that include canines or other living things (with the exception of the human operator) will be considered non-responsive.

- **Performance**

  - Typical boarding team search. Typically only one boarding member will operate the trace detection unit. Small vessel or facility (medium sized yacht - 40 feet and under) equals 4 people (multi-tasking) sweep for about one hour. Large vessel or facility (e.g. marine terminal) equals 4 people (multi-tasking) sweep for about 6 hours.

  - Explosive type. The trace detection unit must provide a capability to detect and identify explosives: nitro-based explosives (required) and peroxide- and chlorate-based explosives (desired).

  - Sensitivity. The trace detection unit must detect and identify explosives contamination at the nanogram level.

  - Interferant conditions. The trace detection unit must detect and identify explosives in the presence of interferants including, but not limited to: fertilizers, household cleaners, adhesives, sodium hydroxide, ammonia, petroleum products, kerosene, ethylene glycol (anti-freeze), household chlorine bleach, engine exhausts, burning fuels, other burning materials, insecticides, and insect repellents.

  - Detection. The trace detection unit must provide on-scene sample collection, analysis, and results indication in less than one minute. Standoff sample collection is preferred, but contact sample collection is acceptable.

  - Power source. The trace detection unit must sustain operations without power replacement for 8 hours. Recommended batteries include off the shelf 9Volt, C, or AA and/or rechargeable versions.

  - Operating conditions. The trace detection unit should operate in a temperature range between -20 degrees Celsius to 50 degrees Celsius and relative humidity between 40% and 93%. The trace detection unit must be able to alert and inform the operator regardless of the lighting conditions, ranging from low/no light environments to direct sunlight.

  - Data Transfer. Wireless data transfer [e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.x] is desired between the trace detection unit and other boarding team members on the boarded vessel or to personnel on a

[1] *S&T Clarification: Proposed options should be described in the offeror's proposal as separately-costed optional tasks.*

FINAL

remote support vessel. Although this capability is not required, preference is given to proposed designs including this capability.

- Probability of Detection. The trace detection unit must provide a probability of detection (Pd) of greater than 0.90 and a false alarm rate (FAR) less than 0.05. However, much higher Pd's and much lower FARs are desired and preference will be given to proposals that realistically project these improved rates.

- Operator Safety. The trace detection unit must be safe for operator use and must meet appropriate safety standards for operation.

- Explosive Atmosphere. The trace detection unit must not cause ignition of an ambient-explosive-gaseous mixture with air (i.e., intrinsically safe in explosive atmospheres). Reference Underwriters Laboratories (UL) 913 (see below) for additional requirements. While the prototype will not be required to meet this standard, the production trace detection unit must.

- Any field calibration, if required, must be accomplished within the setup time (or separately during routine maintenance) without any specialized instrumentation.

- **Configuration and Portability**
  - The trace detection unit must be portable by a single individual wearing and/or carrying the complete unit, and must not require the use of more than one hand to operate. The complete unit must include sample collection, analysis, and results display.

  - The complete unit must weigh less than 10 pounds; less than 5 pounds is desired.

  - The trace detection unit must be able to be carried up and down ladders on a ship and/or transported via vertical insertion from a helicopter.

  - The trace detection unit configuration must be such that it does not interfere with typical maritime environment boarding team operations.

  - The trace detection unit must operate on rechargeable/replaceable battery power (on shore) using both 24-volt direct current (DC) and 110-volt alternating current (AC) power, but must also be capable of supporting operations for up to 8 hours on a self-contained rechargeable power supply, and must include easily replaceable power supplies to enable hot swapping for continuous operations in high-use conditions.

- **Standards**
  - Must meet appropriate safety standards for safe operation.
  - Must meet Hazards and Electronic Radiation to Ordnance (HERO) safety standards (www.tpub.com/content/fc/12404/css/12404_52.htm) if applicable.
  - Must be intrinsically safe per UL 913.

FINAL

- **The prototype should be designed so that the production system meets the following cost goals:**

  (1) A production unit cost of less than $30,000 per unit is desired in production runs of 100.

  (2) Consumables (e.g., filters, reactive agents, batteries) required for operation and routine maintenance of the production system (if any) should be minimal, and should not exceed 5 percent of the unit cost per year of routine operations.

  (3) The production system should not require extensive factory level maintenance. If factory level maintenance is required, it must not normally be required at a greater frequency than one time every three years, and should not cost over 10 percent of the total unit cost.

- **Training Requirements**
  - The contractor shall provide a training package (not to exceed 12 hours) that includes hands-on field training on the equipment for up to eight different sites. Training package learning objectives will include sample collection/survey techniques, detection/identification result interpretation, and false alarm likelihood checking procedures.
  - The prototype must be designed so it is sufficiently easy to operate such that MSST personnel (i.e., high school-educated with knowledge of tactical deployment in a law enforcement environment and who may or may not have training on various types of explosives) following initial training (not to exceed 12 hours) can safely and effectively operate the system.

- **Field Conditions for Use**

  The trace detection unit must be compatible with the following field conditions:

  - Expected operational environments include onboard vessels (e.g., pleasure craft/yachts, cargo vessels, container vessels) and facilities.
  - Resistant to salt and fresh water spray.
  - Trace detection unit must survive transportation onboard small open vessels in 6 to 8 foot seas and transportation to a sea vessel via aircraft (both fixed and rotary wing). Trace detection unit operation will be in relatively calm conditions (moderate-to-low vibration and acceleration conditions).
  - The trace detection unit must be sufficiently rugged to enable operations inside of vessels and buildings, and sufficiently water resistant to operate safely and effectively in various outdoor climates.
  - The trace detection unit must be designed to enable storage in both indoor (e.g., office) and outdoor (e.g., aircraft, maritime vessels, and vehicles) environments.

Users

- United States Coast Guard, Office of Homeland Security Operations and Tactics (G-OPC)
- Customs and Border Protection (CBP)
- State/Local Law Enforcement (LE)

FINAL

- Other Government Agencies (OGA)

Deliverable(s)

Interim Deliverables:

(1) Preliminary design review (estimated within 2 months of program start); the design must be accepted by the government before prototype development.
(2) Critical design review; the design must be accepted by the government before prototype fabrication.
(3) Results of laboratory tests
(4) Test plan for the Preliminary Test
- The contractor shall identify any prototype characteristics that might lead to unsafe operating conditions during the test (e.g., UL 913)

(5) Three (3) Preliminary Test trace detection units
(6) Preliminary Test report
(7) Training and training materials as outlined above

Final Deliverables:

(1) Final Report, including feedback from all testing phases
(2) Prototype documentation (e.g., operating and maintenance manual, troubleshooting guide)
(3) Life cycle cost estimate outlining all procurement, maintenance, and repair costs for the prototype.
(4) Five (5) prototype trace detection units [three (3) may be upgraded from preliminary test units] and related consumables required to enable government-designated personnel to participate in operational field evaluations, which will assist the government in determining follow-on end-item/procurement requirements.

Testing[2]

- **Lab Test**

The contractor shall demonstrate prototype capabilities against stated requirements. If government-furnished explosives (simulated or real) are required, the bidder should so state in the proposal.

- Key elements to be tested are:
  - Probability of Detection/per explosive type (at various ranges from contact to 5 meters)
  - False positive and negative detection rates
  - Interferant testing

- **Preliminary Test**

The contractor shall develop a test plan in cooperation with government Subject Matter Experts (SMEs). The contractor shall provide training for up to 10 users who will operate the prototype during the test. The government will conduct preliminary tests at one location with the technical assistance of the contractor. The testing time is not expected to

[2] *S&T Clarification: For lab, preliminary, and operational tests, testing methodology will depend on detection approach, with standoff-type prototypes being tested at various ranges, and non-standoff prototypes tested on collected samples.*

FINAL

exceed two weeks, including training. The government will provide sample explosives (simulated or real) for the tests. The contractor shall capture test results in the Preliminary Test report including first-hand constructive feedback from the end user and any shortfalls in the prototype's operations.

- Key elements to be tested are:
  - Probability of Detection/per explosive type at various ranges from contact to 5 meters
  - False positive and negative detection rates
  - User interface evaluation (i.e., weight, operated by gloved hand, light conditions, user friendly)
  - Interferant testing
  - Wireless capability (if applicable)

- **Operational Tests**

Operational tests will be conducted by MSST personnel and with other government agencies as observers, (e.g., Customs and Border Patrol personnel) at one field location of the government's choosing. The testing is expected to occur over a one-week period. Minimal on-site participation of the contractor is anticipated.

- Key elements to be tested are:
  - Probability of Detection/per explosive type at various ranges from contact to 5 meters
  - False positive and negative detection rates
  - User interface evaluation (i.e., weight, operated by gloved hand, light conditions, user friendly)
  - Interferant testing
  - Wireless capability (if applicable)

FINAL

3.1.1.2 EC2 – Non-invasive Portable Object Examination System

Descriptive Title:
Non-Invasive, Portable Object Examination System

Note: Proposals that include canines or other living things (with the exception of the human operator) will be considered non-responsive.

A portable capability is required to enable Explosive Security Specialist (ESS) and Bomb Appraisal Officer (BAO) personnel to:

- Assist in the "triage" of objects of interest that emerge during periods of heightened threat conditions and special security event support;
- Screen incoming mail packages in support of their Field Office and headquarters facilities;
- Effectively train security personnel on Improvised Explosive Device (IED) component and IED threat recognition.

For additional detail, please see the section "Background" at the end of this document. In addition, key terms are defined in the section "Glossary" and acronyms are defined in the appendix titled "Acronym List."

The contractor shall develop a prototype demonstrating improved capabilities to examine objects of interest and assist the operator in determining whether they are suspect devices[3]. The contractor shall use an iterative development and testing approach, working closely with the government. The contractor shall include in the proposal two options[4]: one for follow-on testing prototypes in lots of 50 or more, and a second for operational support of prototype units in the field. During this project, the contractor shall develop a prototype to meet the following characteristics:

Description & Specifications:

- A multi-sensor, person-portable prototype to assist trained users (as defined below) in expedient, non-invasive examination of unattended bags, mail packages, and other objects of interest to decide whether the object of interest is a suspect device.

  - **Performance:**

    (1) The prototype must operate remotely when initiated by the user to gather key elements of information on the internal contents and materials composition of an object of interest. Output information that the prototype must provide includes, but is not limited to:

    - Digital image: Multi-aspect, 2-dimensional and 3-dimensional digital images of internal contents;
    - Material density: An indication (i.e., visual display) of material densities that are inherent in the internal contents of the object of interest;
    - Chemical properties: Chemical properties of particulate matter present on the external surfaces of the object of interest, and/or in vapors that may be emanating from the object of interest or its internal contents.

    (2) Prototype output (e.g., imagery, density, chemical and other data) must be displayed to the trained user in a manner that can enable determination as to whether or not the contents or an object of interest should be classified as a suspect device, which for the purpose of this prototype is intended to mean an Improvised Explosive Device (IED).

    - Automated indicator: A desired capability would integrate a red light/green light indicator(s) display for each of the above three information elements without human intervention to alert operators of characteristics that may indicate that the object of interest contains explosives or explosive device components/configurations.

    (3) The prototype must provide output (e.g., data, video) in a commercially accepted format such that it can be transmitted via available communications

[3] *S&T Clarification: The described prototype should assist the operator to determine if the object of interest is a suspect IED; the prototype itself should not make the final determination.*

[4] *S&T Clarification: Proposed options should be described in the offeror's proposal as separately-costed optional tasks.*

systems to prospective responders (e.g., bomb squads) to improve response safety and efficiency[5].

(4) The prototype must produce adequate sensor performance to be capable of penetrating the outer container of a soft-skin object of interest (e.g., backpack, luggage piece) or hard, thin-skinned object of interest (e.g., metal briefcase, ammunition can).

(5) The prototype must be capable of detecting and displaying, in recognizable form, shapes of internal contents, including an 18-gauge wire and a 2-3/4-inch x 3-inch x 1/16-inch printed circuit board housed behind a ¼-inch steel plate within the object of interest.

(6) The prototype, in a single placement, must be designed to interrogate a 4-inch x 12-inch x 18-inch object of interest at the location and in the position in which the object of interest was found, and to allow the user to examine information displays from a distance of at least 100 feet away from the object of interest.

(7) Any field calibration, if required, must be accomplished within the setup time [see (4) under Configuration] or separately during routine maintenance, without any specialized instrumentation.

(8) The prototype must be capable of presenting 2-dimensional and 3-dimensional multi-aspect images that enable the user to correctly ascertain the spatial arrangement of the contents within the object of interest.

(9) The prototype must display material densities (e.g., explosives, steel, aluminum, plastic, food, paper, other materials) in a manner that allows the user to make comparisons between the composition of contents within the object of interest.

(10) The prototype must provide the user with a positive indicator (e.g., colorimetric, electronic) of the presence or absence to the tens-of-nanograms levels of nitrogen-, peroxide-, and chlorate-based materials that may be present on the external surface of the object of interest. A probability of detection (Pd) of greater than 0.90 and a false alarm rate (FAR) of less than 0.05 is desired.

(11) The prototype must be easy to operate after a minimal amount of initial training (not to exceed 24 hours).

(12) Potential future enhancement could include integration on a robotic platform.

- **Configuration:**

  (1) Portability. The prototype must be sufficiently small in size and weight (required less than 168 pounds, desired less than 100 pounds) such that all subcomponents can easily be moved to the object of interest by one person

[5] *S&T Clarification: The output type of the prototype should be of a format (digital and/or video) available for quick distribution to other authorities.*

(wheeled/integral dolly-type container is acceptable) in one trip, maneuvering easily through a standard 36-inch x 80-inch door without external dollies or material handling equipment. Portability attributes are important to enable the user to gain access to objects of interest in small spaces, and to use elevators and normal personnel passageways, doors, etc.

(2) Operator Safety Standoff. The prototype must be safe for operator use and designed to allow the operator to remain at least 100 feet from the object of interest being examined. The prototype must meet appropriate safety standards for human operations.[6]

(3) Expediency. Less than two minutes should be required for placement of prototype components adjacent to, or in close proximity to the object of interest, and for set up of components at the standoff location.

(4) Total prototype setup time. Total time to break out and set up the prototype including both the components at the object of interest, and those at the display/examination site (100 or more feet away), from the time of arrival at the scene until the point in time at which the prototype is ready for initiation by the user, should not exceed 10 minutes.

(5) Space Constraint. The components designed for placement in the immediate vicinity of the object of interest must fit within 16 square feet (i.e., 4 x 4-foot square or a 2.2-foot radius circle) of area surrounding the device.

(6) Power source. The prototype must be able to operate on both internal and external power capability. The prototype must be capable of operating off of both 24-volt DC and 110-volt AC power, but must also be capable of supporting operations for at least 2 hours on a self-contained rechargeable power supply. The prototype must include easily replaceable power supplies to enable continuous operations for up to 16 hours in high-threat conditions.

(7) Data storage and search. The prototype must be capable of tagging prototype output with user-entered data (e.g., item description, time/date, location). The prototype must enable keyword searches against historical data for analysis and training functions.

(8) Processing time. The prototype must be capable of processing and displaying information on objects of interest within three minutes of system initiation by user for soft-cased objects of interest, and within five minutes of system initiation by user for thin, hard-cased objects of interest. Time from "system initiation" is defined to be the time from the original turn-on of the system, not from standby mode.

- **The prototype should be designed so that the production system meets the following cost goals:**

[6] *S&T Clarification: Appropriate safety standards for the proposed technologies or devices.*

(1) A production unit cost of less than $120,000 per unit is desired in production runs of 50 units.

(2) Consumables (e.g., filters, reactive agents, batteries) required for operation and routine maintenance of the production system (if any) should be minimal, and should not exceed 3 percent of the unit cost per year of routine operations.

(3) The production system should not require extensive factory level maintenance. If factory level maintenance is required, it must not normally be required at a greater frequency than one time every three years, and should not cost over 10 percent of the total unit cost.

Training requirements:

(1) The contractor shall provide a training package (total not to exceed 24 hours training time) that includes hands-on training on the equipment at up to two user locations for field testing. Training may be computer-based, instructor-based, or a combination of the two.

(2) The prototype must be designed so it is sufficiently easy to operate such that ESS and BAO personnel (i.e., personnel who already possess training in recognition of objects of interest to be examined), following initial training (not to exceed 24 hours), can safely and effectively operate the prototype.

Field conditions for use:

(1) The production system must be sufficiently rugged to enable operations inside of buildings and should be sufficiently water resistant to be operated safely and effectively in various outdoor climates (e.g., -20 degrees Celsius up to +50 degrees Celsius air temperature, high humidity, light drizzle or rain conditions).

(2) The production system must be designed to enable storage in an indoor (e.g., office) and outdoor (e.g., vehicle) environment.

Users:

- Immigration Customs and Enforcement (ICE)
- Explosives Security Specialists (ESS) within the Department of Homeland Security
- Bomb Appraisal Officers currently assigned within the Transportation Security Administration (TSA) screening force
- Other Federal, State, and Local Law Enforcement and physical security

Deliverables:

Interim Deliverables:

FINAL

(1) Preliminary design review (estimated within 2 months of program start); the design must be accepted by the government before prototype development.
(2) Critical design review; the design must be accepted by the government before prototype fabrication.
(3) Results of laboratory tests.
(4) Test plan for the Field Test.
(5) Three (3) Field Test prototypes.
(6) Field Test report.
(7) Training and training materials as outlined above.

Final Deliverables:

(1) Final Report, including feedback from all testing phases.
(2) Prototype documentation (e.g., operating and maintenance manual, troubleshooting guide).
(3) Life cycle cost estimate outlining all procurement, maintenance, and repair costs for the prototype.
(4) Three (3) prototypes (upgraded from field test systems) and related consumables are required to enable government-designated ESS personnel to participate in operational field evaluations, which will assist the government in determining follow-on end-item/procurement requirements.

Testing:

- **Lab Test**

The contractor shall demonstrate prototype capabilities against stated requirements. The government will provide 20 sample objects of interest.

- **Field Test**

The contractor shall develop a test plan in cooperation with government Subject Matter Experts (SMEs).The contractor shall provide training for up to 10 users who will operate the prototype during the test. The operators should be trained to a level that they can train additional personnel as a mobile training team during operational tests. The government will conduct a field test at a single location with the technical assistance of the contractor. The test is not expected to exceed two weeks. The government will provide the sample objects of interest for the tests. The contractor shall capture test results in the Field Test report including first-hand constructive feedback from the end user and any shortfalls in the prototype's operations.

- **Operational Tests**

Operational tests will be conducted by ESS personnel at government field offices. The mobile training team will provide training to the ESS personnel. No participation of the contractor is anticipated on-site, but reach back technical assistance and support shall be available. All Operational tests are expected to occur over a one-month period and may occur simultaneously.

Key Elements of Field and Operational Tests include:

- User feedback

FINAL

- All requirements identified above with an emphasis on the following key performance parameters:
  - Characterized Pd and FAR thresholds for chemical detection for soft- and hard-skinned objects of interest.
  - General performance against 20 government-provided sample objects of interest.
  - Prototype setup time.
  - Prototype data collection and processing times.
  - Ability of prototype output data to be transmitted via commercially accepted format.

Glossary:

Trained User – An Explosives Security Specialist (ESS) or Bomb Appraisal Officers (BAO) with prior training as a bomb or EOD (Explosive Ordnance Disposal) technician who works in a prevention capacity and not as a responder.

Object of Interest – A package (e.g., handbag, backpack, luggage, mail parcel) where limited information on its origin is discovered and impedes operations that warrants further investigation. It does not yet constitute a suspect device.

Suspect Device – An object of interest that has been identified as a threat improvised explosive device (i.e., by examination, hoax, call-in) that requires a response.

Non-invasive – Implies a method whereby no significant additional movement of the object of interest is required. The object's position and attitude should not be changed, and the object should not be required to be moved from the location in which it is found. Swiping actions on the external surfaces would be permissible, provided the shape in which it is found is not altered, and provided that swiping activities do not exert any appreciable weight on any of the external surfaces (e.g., less than 20 grams of force) of the object.

Background:
Portable, field X-ray units currently in service by bomb squads in the United States, Department of Defense EOD teams, and other activities, do not have multi-sensor capabilities, and are limited in processing and displaying attributes of objects of interest. This makes timely decision making difficult. Many of these units lack digital imaging capabilities, and lack 3-dimensional processing and display, or multi-sensor capabilities.

Airport detection and screening systems [e.g., Walk Through Metal Detection (WTMD), Explosives Detection System (EDS), Trace Detection] are designed for operation at checkpoints, as relatively large, fixed stations. These systems are frequently operated for long periods of time to process a relatively high volume of personnel and luggage through security checkpoints. Because of these high throughput systems, discovery of unattended or unclaimed items can disrupt security and screening/checkpoint operations, especially during periods of heightened security. Without more information on the contents of an object, this often proves disruptive and costly in terms of facility and personnel down time while waiting for an object declared to be a suspect device because incomplete information has to be cleared by appropriate authorities.

FINAL

Furthermore, processing of objects through checkpoint screening equipment may require the object to be carried a considerable distance with virtually no information on the internal contents and possibly placing personnel at risk.

Trained Explosive Detection K-9 units offer an effective means of searching areas for suspect materials, but they cannot and should not be employed to "clear" a suspect device.

Integrating multiple sensors and incorporating advanced processing techniques into a highly portable field system, and characterizing performance of that system against small objects of interest for operation by trained users within the Federal Air Marshal Service (FAMS) and Transportation Security Administration (TSA), with technical knowledge and skills from prior EOD/bomb squad experience can enhance operational safety, improve efficiency, and aid in threat mitigation during periods of increased threat.

ESS personnel currently assigned within the FAMS, and Bomb Appraisal Officers (BAOs) within the TSA are all either formerly qualified DoD Explosive Ordnance Disposal (EOD) technicians, or bomb technicians with hazardous device school training and prior operational experience in explosives and explosive component devices. These personnel today possess no organic capability to examine objects of interest beyond simple, external examination. During periods of heightened threat conditions, ESS personnel are often called upon to support bomb management and incident management centers to offer expertise and assistance to decision makers on IEDs, without detracting from response bomb squads that are often stretched thin during incidents and security events. Most bomb squad response activities occur today against items that with a fundamental examination capability could have been eliminated before elevating to the status of a suspect device. During these support operations, a means to quickly triage packages, unattended bags, and other objects of interest to assist in focusing bomb squads on items where their response capability is genuinely needed. ESS personnel also play a continuing important role in training FAMS personnel and collaborating security forces in explosives and explosive device recognition to deter and prevent IED incidents in the aviation and other transportation modes.

3.1.1.3 EC3 – Advanced Capability X-ray System for Bomb Squad

Descriptive Title:
Advanced Capability X-ray System for Bomb Squad

The contractor shall develop a prototype demonstrating improved capabilities to perform diagnostics of Improvised Explosive Devices (IEDs). The contractor shall use an iterative development and testing approach, working closely with the government. The contractor shall include in the proposal two options[7]: one for prototypes in lots of 100 for testing, and a second for operational support of prototype units in the field. During this project, the contractor shall develop a prototype to meet the following characteristics:

Description & Specifications:

[7] *S&T Clarification: Proposed options should be described in the offerors's proposal as separately-costed optional tasks.*

- The Advanced Capability X-ray System must provide the user with improved penetration and resolution to conduct radiographic examination and diagnostics of suspected packages and confirm the presence of an improvised explosive device (IED).
- The government prefers that the prototype and the production system do not require the use of a radioactive source. Should any source be required to conduct diagnostic operations the responsibility for obtaining the necessary licensing and certification for all units will be the responsibility of the manufacturer.
- The prototype must be able to handle targets up to 3 feet x 3 feet x 18 inches (depth).
- The X-ray unit and all accompanying components necessary for conducting diagnostic operations must be of a volume and weight that a single operator (e.g. bomb technician) can carry and deploy the necessary items to the incident site from the designated safe area while the operator is in the approved safety ensemble.

Performance:

(1) The prototype must be command operated; all operational controls must be able to be remotely operated by the bomb technician in order to garner necessary information and contents of an IED.

(2) The prototype must function in the same manner consistent with existing portable transmission X-ray systems, while providing enhanced capabilities by improving the ability to penetrate substances and materials typically found or associated with IEDs.

(3) The images captured from a suspected IED must have enhanced resolution to the level that exceeds current standards and provides clear and concise images of the contents within the package. This enhancement may either be through hardware and/or software improvements.

(4) The above two are the critical characteristics of the improved prototype and therefore preference will be given to proposed prototypes showing the greatest improvement.

(5) The prototype must be compatible and interface with current and accepted e-mail systems. In addition, use of a Universal Serial Bus (USB) port to provide the capability for downloading data files is required. The prototype must provide a wireless capability [e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.X] to communicate data and images to/from other response organizations in reach back mode.

(6) The X-ray system's image plane (X-ray receiver) must be adaptable to operate in various configurations and provide the capability to insert the image plane within a space of not more than 0.5 inches without disturbing the IED. The material used must be lightweight in order to facilitate the need for suspending the image plane or placement in an elevated location[8].

(7) The prototype must provide the following ergonomic characteristics: robust in design and durable for use in conditions involving inclement weather and adverse environmental conditions (e.g., sandstorms).

Configuration:

(1) The prototype must be stored in a suitable transport case(s) to aid in mobility of the system and allow for ease of transport of the system during stressful operations and difficult conditions.

[8] *S&T Clarification: The imaging plane of the device (if used in a transmission-type mode) should be able to fit within a planar space, between the IED and another object (e.g., a wall), of no more than 0.5 inches wide.*

FINAL

(2) The X-ray system must be versatile enough to be mounted and operate on a broad range of robotic platforms (consistent with bomb squad operations) while maintaining the capability to be operated remotely.
(3) The prototype must be capable of tagging system output with user-entered data (e.g., item description, time/date, location). The prototype must enable keyword searches against historical data for analysis and training functions.

Cost Considerations:

(1) The target unit cost for the production system should be comparable to existing portable X-ray systems in bomb squad inventories. The proposal must include an estimated cost of production units in quantities of 100. Training requirements and costs for the production system must be incorporated in the estimated cost. Maintenance support and warranty should be included in the estimated cost of the production system.

Training Requirements:

(1) The contractor shall provide written material describing the prototype and its operations.
(2) The contractor shall provide training during field trials sufficient to allow the operators to safely and effectively operate the prototype.

Field conditions:

(1) Response agencies are subject to operate under a number of stressful and adverse conditions and inclement weather. Therefore, the prototype must be designed to withstand a number of demanding operational conditions. The prototype should be designed to function in temperature ranges of -29 degrees Celsius to +54 degrees Celsius.
(2) The prototype must be robust in design, which allows for operating in rough terrain (desert, tropical and wet weather) and must withstand rough handling in transport.
(3) The government prefers a design that is compatible with military operations in order to leverage the Department of Defense (DoD) market.

Users:

- Protective Security Division-Weapons of Mass Destruction (PSD-WMD)/Bombing Prevention Unit in the Department of Homeland Security
- State and Local bomb squads
- DoD EOD (Explosive Ordnance Disposal) units

Deliverables:

Interim Deliverables:

(1) Preliminary Design Review (estimated within 2 months of program start); the design must be accepted by the government before prototype development.
(2) Critical Design Review; the design must be accepted by the government before prototype fabrication.
(3) Results of laboratory tests
(4) Test plan for the preliminary field test
(5) Three preliminary field test units of the Advanced Capability X-ray System
(6) Preliminary field test report

FINAL

Final Deliverables[9]:

(1) Final Report, including prototype description and operations.

(2) Six operational test units of the Advanced Capability X-ray System, including all required accessories and consumables. The contractor may choose to upgrade the three preliminary field test units to satisfy part of this requirement.

Testing:

Lab Tests:

(1) The contractor shall demonstrate prototype capabilities compared to existing systems[10]. The government will provide one or more targets to be used for the comparison tests.

Preliminary Field Test:

(1) The contractor shall develop test criteria incorporating guidance from the Bombing Prevention unit and select government Subject Matter Experts (SMEs) to assist prescribing necessary parameters. The contractor shall provide training for up to 10 users who will operate the prototype during the test. The operators should be trained to a level that they can train additional personnel as a mobile training team during operational tests. The government will conduct a field test at a single location with the technical assistance of the contractor. The test is not expected to exceed two weeks. The government will provide the target devices (real or simulated IEDs) for the tests. The contractor shall capture test results in the Preliminary Field Test report including first-hand constructive feedback from the end user and any shortfalls in the prototype's operations.

Key Elements to Consider for Preliminary Field Testing:

(1) User-acceptable human factors and system interface.

(2) Efficacy against simulated and/or real IEDs.

(3) Efficacy against a number of containers and a variety of materials that can be used for housing an IED.

Operational Tests:

(1) Operational tests will be conducted by bomb squads at three major metropolitan cities. The mobile training team will provide training to the bomb squads. No participation of the contractor is anticipated on-site, but reach back technical assistance and support shall be available. All three Operational tests are expected to occur over a one-month period and may occur simultaneously.

FINAL

9 *S&T Clarification: Final deliverables should also include Prototype documentation (e.g., operating and maintenance manual, troubleshooting guide) and lifecycle cost estimate outlining all procurement, maintenance, and repair costs for the prototype.*

10 *S&T Clarification: The proposer shall demonstrate prototype capabilities compared to published results of existing commercial systems. No testing or acquisition of existing systems is required.*

3.1.2 Biological Countermeasures (BC) Topics:

3.1.2.1 BC1 – Rapid Suspected Bio-agent Screening

Descriptive Title:
Rapid Suspected Bio-agent Screening (tool kit which eliminates the probability of biological threat agents)

Description & Specifications:

- The contractor shall develop a tool and method for rapidly screening suspicious "white powders" to eliminate the probability that the substance is a biological threat agent. The goal is to be able to distinguish between biological threats and common white powdery substances. The contractor shall provide test data confirming the performance of the prototype within the parameters listed below.

  - Performance:
    - Provide a quick and reliable method to eliminate the probability that a substance is a biological threat agent.
    - The output should be either a positive or negative.
      - A negative indicates that the material is *not* a biological threat agent.
      - A positive *does not* indicate with absolute certainty that the powder *is* a biological threat agent. Additional confirmatory tests will be required, which is outside the scope of this task.
    - For that reason, the tool must not show a positive indication for any of the following powdered substances (*Note: simple proteinacious tests alone are not sufficient to meet this requirement*):
      - coffee creamer
      - sugar and sugar substitutes
      - flour
      - foot and talc powder
      - dry wall dust
    - The government will give preference to proposed approaches that expand the above list while meeting the stated intent of the product.
    - Tool is for screening only; it does not need to identify the material being inspected.
    - Test must be complete within 5 minutes.
    - Tool must include means for positive control to ensure viability of the test.
    - Must not require individual using tool to make direct physical contact with the suspicious material. Contact if necessary may be accomplished via use of probes, swabs, or other sampling approaches.
    - Tool must not reaerosolize particles during test process and disposal of tool.

  - Configuration:
    - Hand held, lightweight
    - Shelf life should be at least 5 years, and stored at temperatures ranging 0 degrees Celsius – 60 degrees Celsius without degradation of product.

FINAL

- Tool must not be hazardous material (HAZMAT) as packaged, and must not require handling as hazardous waste (HAZWASTE) when disposing unused quantities (i.e. no decontamination daughter products present).
- Tool must be capable of reliable function from Sea Level to 10,000' Mean Sea Level (MSL).
- Tool and packaging must not present a hazard during rapid decompression from 8,000' MSL to 40,000' MSL equivalent.
- Tool must be intrinsically safe.

- Cost Considerations:
  - The prototype should be designed so that the final product unit cost should not exceed 20 dollars (goal of $1 per test) based on quantities of 5,000.

- Training Requirements:
  - No training required. Labeling instructions will suffice. Proper use should be intuitive.

- Field Conditions for Use:
  - Commercial aircraft cabins, Airline terminals, office buildings
  - Tool should be effective from 0 degrees Celsius – 40 degrees Celsius.

Users:

- Transportation Security Administration (TSA), Federal Protective Service (FPS)
- Airline industry, commercial facilities

Deliverables:

- Interim deliverable: 100 prototype units for field testing
- 100 sample units
- Test plan and data to support validation of effectiveness.
  - Live agent test data
  - A statistically significant evaluation of detection and false positive rates against the specific materials listed above
  - Developmental testing is responsibility of vendor
  - System Safety Assessment

Field Testing:

- The contractor shall deliver 100 prototype kits to the government for use in field testing by government users. The focus of these tests will be ease of use, configuration of packaging, and efficacy against known threat agents or surrogates. The government will provide feedback on those tests for improvement of the final deliverable. Participation by the contractor in the field test is not required, nor desired.

3.1.2.2 BC2 – Aircraft "Spot" Decontamination

Descriptive Title:

FINAL

- Aircraft "Spot" Decontaminant [Aerospace Material Specification (AMS)-1453, Military Standard Performance Specifications (MIL-PRF)-85570, or equivalent materials compatibility].

Description & Specifications:

- The contractor shall develop a kit and method for use to provide "Spot" decontamination of common aircraft cabin materials. The contractor shall perform all testing required to confirm the performance of the product within the parameters and specifications listed below. The contractor shall provide the test data to the government as part of the final deliverable.

Performance:

- Neutralize the effects of biological agents in an aircraft cabin environment on the ground or in-flight. This can be done through deactivating the agent, safe removal of the agent or any other method to achieve the desired outcome.
- No adverse effects to aircraft and aircraft systems due to application of product and resulting effluent streams from the decontamination process.
- Should be effective against biological agent threats: *Bacillus anthracis (vegetative and endospores),* Smallpox virus, Ebola virus, *Salmonella typhi*, *Yersinia pestis*, Ricin, *Clostridium botulinum,and* botulinum toxin
- Demonstrate 6-log reduction in stated biological challenge [per Environmental Protection Agency (EPA) testing protocol] for *Bacillus anthracis (vegetative and endospores), Yersinia pestis*, Ricin, *Clostridium botulinum, and* botulinum toxin.[11]
- Shall provide for effective decontamination of a minimum area of one square meter over common aircraft cabin interior porous and non-porous substrates.
- Decontaminant should be effective from 0 degrees Celsius to 60 degrees Celsius.
- Five (5) year shelf-life in ready-to-use packaging.

Configuration:

- Material must be packaged ready-to-use, with intuitive instructions printed on the packaging.
- Material must not be HAZMAT as packaged, and must not require handling as HAZWASTE when disposing unused quantities (i.e. no decontamination daughter products present).
- Packaging must provide adequate protection / not present a hazard to personnel in the event of rapid decompression from 8,000' Mean Sea Level (MSL) to 40,000' MSL equivalent.
- Single use packaging must not exceed 18 linear inches, with the objective of minimizing package volume and weight.
- Material and packaging must be intrinsically safe to handle and use.

Standards (as applicable):

- Disinfectant Cleaner for Aircraft Interior General Purpose Liquid, AMS-1453
- CLEANING COMPOUND, AEROSPACE EQUIPMENT, MIL-PRF-87937

[11] *S&T Clarification: Tests and resulting data to be provided by bidder, or bidder may request as part of its GFI portion of the proposal that the government perform the test.*

- CLEANING COMPOUND, AIRCRAFT SURFACE, MIL-PRF-85570
- Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA)

Cost Considerations:

- The prototype should be designed so that the final product unit cost should not exceed 20 dollars per use based on quantities of 5,000.

Training Required:

- No training should be required prior to product use. Product use instructions should be clearly marked on packaging.

Field conditions for use:

- Aircraft cabin environments

Users:

- Transportation Security Administration (TSA)
- Commercial aviation
- Airline Industry
- Department of Defense Joint Program Executive Office for Chemical and Biological Defense

Deliverables:

- Interim deliverable: 50 prototype kits for field testing
- 100 sample spot-decon 'units'[12]
- Recommendations for completion of EPA registration[13]
- Live agent test data to confirm efficacy
- Test data to confirm compliance with one of the following AMS-1453, MIL-PRF-87937, or MIL-PRF-85570

Field Testing:

- The contractor shall deliver 50 prototype kits to the government for use in field testing by government users. The focus of these tests will be ease of use and configuration of packaging. The government will provide feedback on those tests for improvement of the final deliverable. Participation by the contractor in the field test is not required, nor desired.

3.1.2.3 BC3 – Biosurveillance Detection Algorithms

Descriptive Title:

- Biosurveillance Detection Algorithms

[12] *S&T Clarification: In total, while performing, the offeror should provide 150 test kits: 50 during an interim stage for government testing, and 100 additional units prior to the completion of the contract.*

[13] *S&T Clarification: 'Recommendations for completion of EPA regulations' should be interpreted to indicate that the performer will provide a plan to allow for completion of the EPA testing obligations.*

FINAL

Description & Specifications:

- The contractor shall develop algorithms implemented in modular software packages to improve our biosurveillance capability.

Performance:

- Develop an algorithmic procedure/model to provide earliest detection of bioterrorist attacks on humans, plants, animals, food, water, or the environment based on correlations between a broad range of low confidence biosurveillance data streams.
    - In this context *detection* means an increase in the likelihood that an event has taken place and may trigger deeper analysis to arrive at a conclusion.
- Correlations between data streams should take into account the time lags associated with the various modes of terrorist attack and data reporting, including: a broad range of known pathogenic animal and human, plant, food-borne micro-biological organisms, including viruses, bacteria, fungi and rickettsia. *[e.g. Anthrax, Cholera, Plague, Tularemia Q-fever, Ebola-Marburg, (other Hemorrhagic fever), Hantavirus, Hepatitis A, B, & C, Rabies, Smallpox, Venezuelan Equine Encephalitis, Foot and Mouth disease, Brucellosis, Glanders, Melioidosis, Typhoid, Typhus, Q fever, Staphylococcal, Clostridium, simultaneously a broad range of know pathogenic toxins, including proteins as well as other biochemical organic compounds, e.g. Botulinum Toxin, Ricin, Saxitoxin, Staphylococcus Enterotoxin B, Trichothecene Myco-toxins]*
- Must include the ability to receive cues from other external indications and warnings of a possible terrorist attack, including geographic description, tactics, and timing.
- Test in at least one geographic area and successfully analyze cross-sector data without significant false positive results.
- Software package must be modular and adjustable to incorporate new data streams and correlations by the end user.
- Detection algorithms must function with sufficient speed to permit a response in order to mitigate the detected event.
- The contractor must provide support to Department of Homeland Security (DHS) security reviews of the software.

Field Conditions for Use:

- Must work in any UNIX-based computer environment.
- Must be implemented in a modular fashion in a service-oriented architecture.

Users:

- Information Analysis/Infrastructure Protection (IA/IP)
- All other government agencies participating in the biosurveillance program.

Deliverables:

- Fully functional software package including a fully paid-up, royalty-free license with unlimited distribution and data rights
- User manual and reference manual must be provided
- Report of verification and validation plans, data and results
- Copy of the source-code in electronic form
- Critical Design Review

FINAL

Field Testing:

- Iterative development process working closely with the government customer.
- All contractor personnel working onsite with the government must be cleared to the secret level.

3.1.2.4 BC4 – Rapid Field Identification of High Priority Plant Pathogens (RFIP)

Descriptive Title:

- Rapid Field Identification of High Priority Plant Pathogens (RFIP)

Description & Specifications:

The contractor shall develop a person portable prototype that will provide minimally-trained Agriculture users assistance in field identification of plant pathogens. The prototype must be designed to meet the specifications listed below. The intention of the prototype / device is to perform field screening in order to significantly reduce requirements for follow-on laboratory testing. The prototype should perform rapid field identification of plant bio-terrorism agents and pathogens of high consequence including:

- Fungi (e.g., potato wart, brown stripe downy mildew, Philippine downy mildew)
- Fungal-like organisms (e.g. *Phytophthora ramorum*, causal agent of Sudden oak death)
- Bacteria and bacteria-like organisms (e.g., citrus greening disease, bacterial leaf stripe, *Ralstonia solanacearum* race 3 biovar 2)
- Plant viruses.

The government will give preference to proposed approaches addressing the broadest range of these high consequence threat agents and pathogens. The prototype must complete the test in 30 minutes or less. Presently, only visual identification of affected symptomatic plants can be made in the field environment for these microorganisms.

Performance:

- Provide an initial "Red Light / Green Light" in-the-field test[14]. This primary step in identification will reduce the reach back requirements presently encumbering this process.
- Can detect plant pathogens that need field-detection capability, minimally: fungi, fungal-like organisms, bacteria and bacteria-like prokaryotes, and plant viruses.
- Prototype device should be upgradeable with minimal cost to allow addition of other plant pathogens within the above categories as threats may change.
- Presentation of suspect material may be provided to prototype from a small initial sample.
- Decrease false positives going to the lab while simultaneously identifying true positives currently missed.
- Ideally, device will indicate if material presents a threat or not.
- Must be inherently safe.

[14] *S&T Clarification: "Red Light/ Green Light" should indicate the positive or negative detection of an agricultural pathogen respectively. The intent is to produce a device that clearly determines if a product can be shipped.*

- The primary application is to analyze plants or plant products that bear visible anomalies. However, the government will give preference to proposed approaches that can ultimately be used for trace identification.

Usability:

- The prototype must be designed to be used at ports of entry, plant inspection stations, and other environments such as farms and forests.
    - Useable by minimally trained field personnel in a non-laboratory environment.
    - Must be simple to use, either handheld assays, reagents or device.
- Must provide "Go" or "No go" response / indication. "No go" initial screen must be extremely reliable (near 100 % of true positives).
- Cost should be less than $1.00 per sample, and preferably less than $0.50.
- Should be easily portable and set-up friendly.
- Shelf life of consumables (reagents, etc) required: 6 months, preferred: 1 year or more.
- A desired, but not required, characteristic of the prototype is the ability to provide wireless import and export of data to/from standard Personal Computers (PCs) or laptops.
- The prototype must provide audible and visual alerting to detected pathogens. The user must be able to select the alarm mode.
- The prototype must be designed to require minimal training. Users should be able to operate the system based on the user manual or an intuitive interface.

Configuration:

- Operational use in the field in a variety of environments, therefore rugged and robust. High and low temperatures that would be expected in both southern and northern border extremes.

Cost Configuration:

- Low per sample costs based on 100's or 1,000's of samples per month.
- The prototype must be designed in a way that the production system will cost less than $40K in production quantities of 100, significantly lower cost is desired.

Users:

- Customs and Border Protection (CBP) / Animal and Plant Health Inspection Service (APHIS)
- United States Department of Agriculture (USDA)
- Civilian farm sector / Professional farmers
- University and other Agricultural Organizations

Deliverables:

- 4 Prototypes for field testing
- Report of efficacy testing
    - The contactor shall test and report the performance against agents of regulatory significance. If government samples or assistance is required the proposal should so state.

Field Testing:

- Will be performed by CBP/APHIS

FINAL

- The contractor needs to be available to provide up to one day training at the beginning of the field test and should be available onsite for up to a week to provide technical assistance and make observations of field efficacy.

3.1.3 Chemical Countermeasures (CC) Topics:

3.1.3.1 CC1 – NIOSH CBRN 60 Tactical Escape Mask

Descriptive Title:

NIOSH CBRN 60 Tactical Escape Mask

Description & Specifications:

Vendor shall develop a lightweight, one-time use, National Institute of Occupational Safety & Health (NIOSH)-approved tactical escape mask with 60-minute endurance in Chemical Biological Radiological and Nuclear (CBRN) environments meeting the specifications described below. The vendor is responsible for obtaining NIOSH certification. The vendor shall also develop an associated training device.

Performance:

When donned:

- Mask must be capable of 60-minute exposure to CBRN without break through.
- Mask must not severely restrict vision; individual wearing mask must be capable of engaging targets with small arms at ranges up to 50 feet.
- Mask must allow for tactical movement without compromising function (chemical seal, vision, etc).
- Mask must fit over prescription eye glasses.
- Total time from start to finish of donning must be no more than 45 seconds. Estimated time from removal from packaging to start of donning is 30 seconds or less. Estimated time to don is 15 seconds or less.
- Mask must allow for verbal communication (i.e., will not prevent individual wearing mask from speaking or severely reduce hearing).

When carried concealed:

- The mask will typically be carried concealed on an individual for extended periods. Therefore the mask must be protected from common mishandling such as dropping, kicking, stepping and sitting upon, etc.

In storage:

- The mask must not require special storage conditions (e.g., no relative humidity or temperature limits).

Mask lifetime:

- Mask should have a combined storage and concealed use life of at least 5 years.

Configuration:

- Mask must be able to be concealed underneath a conservative male or female sport coat.

FINAL

- Mask and any packaging in ready-to-use configuration must weigh less than 5 lbs and lower is better.
- Any packaging must provide protection to mask from everyday carriage on a user, and occasional accidental water immersion.
- Mask must fit full range of non-bearded adult physiology.

Standards

- NIOSH Escape Mask standards scaled to 60-minute duration in CBRN environment.

Cost Considerations

- Production mask unit must cost less than $200 (threshold) or $100 (objective) in quantities greater than 5000 units.
- Mask must not require additional consumables or maintenance throughout shelf life.

Training Mask Requirements

- Performer must provide rugged, re-useable masks marked clearly "FOR TRAINING USE ONLY" for personnel to train don, doff, and tactical use.
- Training mask must accommodate 100 don/doff wear cycles without reduction in mask integrity.
- Developers shall specify cleaning procedures between uses.
- Training mask must be simple to don and doff, and not require more than annual familiarization training.
- Training mask does not need any protective capability or concealability.

Field conditions for use include the following:

- Mask must be capable of use in full range of both interior environments and exterior environments (e.g., arid desert to humid to cold).
- Mask and packaging must be capable of withstanding frequent cycling to atmospheric pressures equivalent to 10,000' MSL (mean sea-level).
- Mask in packaging must not present a hazard to personnel carrying item during depressurization of an aircraft cabin at 40,000' MSL (mean sea-level).

Users:

- Department of Homeland Security (DHS) / Border and Transportation Security
- DHS / Immigration and Customer Enforcement
- Airline Industry
- State and Local First Responders.

What is (are) the deliverable(s)?

- Interim deliverable for field test: 25 masks for field destructive and non-destructive testing (NIOSH certification not required, but interim prototype deliverable must be reflective of final deliverable with respect to form, fit, and function).
- Proof of NIOSH certification
- Final deliverable: 25 Prototype masks with NIOSH certification and 10 multi-use training masks

FINAL

Field Testing:

The government will perform testing of the interim prototype mask but not of the training mask. Key elements to be tested include:

- Fit and function
- Concealment under conservative business attire
- Qualitative evaluation of "wearability" in concealed use configuration for extended periods (14-hour days, 5 days per week). Wearability includes users' perception of comfort, concealment, durability of packaging under normal use.

The number of prototypes required for field testing is listed in "Deliverables" above.

The vendor shall provide limited participation during field testing. Specifically, minor adjustments to the prototype configuration may be required during and as a result of Field Testing.

3.1.3.2 CC2 – Escape Hood

Descriptive Title:
Escape Hood

General:
The contractor shall develop and validate the performance of a small concealable escape mask[15] that will allow personnel to safely leave potentially contaminated areas. The purpose of the mask is to allow a quick safe withdrawal from the contaminated area, but is not intended to provide extended respiratory protection for first responders.

Protection Time:
The mask shall provide respiratory protection as specified below for a minimum of fifteen (15) minutes.

Form Factor:
The mask shall be packaged in a manner that enables it to easily fit in the inside pocket of a suit jacket (approximate dimensions of 4-1/4" wide x 8-1/2" long x 3/4" deep).

Weight:
The maximum weight of the mask should be approximately one pound.

Protection Level and Validation:
The mask shall filter both particulate matter (to remove biological agents and radiological material) and vapors (to remove chemical agents).

Validation:

[15] *S&T Clarification: Proposed efforts may include both mask and hood-type formats, as long as performance is not impacted.*

The contractor shall validate the performance of the mask to insure that it meets these performance specifications. Tests shall be conducted at an independent laboratory using applicable industry-accepted or Department of Defense (DoD) accepted test protocols. Proposed test methodology shall be provided to the Government for review and approval.

At a minimum, the mask shall effectively filter nerve, blood, and blister agents. Removal of toxic industrial chemicals (TIC's) is desired.

The particulate filtration efficiency of the mask shall meet or exceed the requirements for High Efficiency Particulate Air (HEPA) filters (i.e. removal of a minimum of 99.97 percent of 0.3 micron particulates)

At a minimum, the mask shall provide a protection factor of 1000 (i.e. be able to remove a minimum of 99.9 percent of chemical vapor molecules present in the ambient air).

Resistance to Chemical Attacks:
In order to ensure that the integrity of the mask is not affected if a hazardous material is splashed on it, material compatibility tests shall be conducted. All the materials used in the construction of the mask shall show no signs of failure or penetration for a minimum of twenty minutes when representative hazardous materials are placed directly on the material. Materials stability when in contact with chemicals other than Weapons of Mass Destruction (WMD) agents may be required and specified (e.g. hazardous industrial agents).

Deployment:
Donning the mask shall be quick (less than 10 seconds) and simple. No special modifications to the mask shall be required for users wearing eyeglasses or having facial or upper neck hair. Mask shall allow for verbal communication.

Shelf Life:
The mask shall have a minimum of a three-year shelf life, without any special storage requirements.

Operations Manual:
Instructions on how to use the mask shall be included as part of the outer packaging material of the mask. The instructions shall be written in a font size large enough to be easily read and shall be written in a fade resistance ink to insure that it is still legible at the end of the three year shelf life.

Contractor shall provide inert masks for training sessions. Cleaning instructions for training masks shall be provided.

Manufacturing or Production Capabilities:
In order to insure that these masks will be available by government personnel on a long term basis as required, the contractor shall also have a demonstrated ability to manufacture these masks so they are readily available (i.e. delivery within 90 day of receipt of order) when ordered by the government, or have a transition/licensing plan in place with another contractor that has this capability.

FINAL

Deliverables:
Validation test reports
Mask specifications and capabilities
Operations manual
Cleaning procedures for training sample masks
Five inert masks for training proposes
300 working prototypes for field evaluation

Customer Agency Requirement:
The customer agency shall provide DHS with a Technical Advisor to participate in the technical oversight of this project. This Technical Advisor will ensure that the needs of the customer agency are being met by the contractor and that the deliverables accurately reflect the customer agency's requirements. The Technical Advisor shall be involved in the project's development, including: providing a Statement of Requirement for this task, identifying the appropriate proposals and developers, reviewing the progress reports generated during the course of the project, and attending project review meetings.

3.1.4 Information Technology – Geospatial (ITG) Topics:

3.1.4.1 ITG1 – Transportation Route Risk Analysis and Resource Allocation Tool

Descriptive Title:
Transportation Route Risk Analysis and Resource Allocation Tool

Description & Specifications:
The contractor shall develop a prototype to support transportation route risk analysis. The primary output of the tool will be a list of transportation routes ranked according to relative risk. This output will be used as an input for resource allocation planning.

Performance:
The prototype must serve as an effective decision support and probability-based analysis tool to assist DHS and other appropriate Federal departments in determining relative risk in order to better align resource and manpower deployments to the highest risk routes for protecting critical infrastructure located near a transportation route. The tool must integrate multi-departmental reporting; correlate this information with industry and private sector open-source information as well as geospatial and event data; triangulate this information to key critical infrastructure information; and generate a prioritized risk assessment by applying probability modeling techniques. A capability to aggregate and array inter- and intra-departmental resource and manpower asset support across specific times along particular transportation routes is an essential component of the prototyping effort.

The initial prototype will concentrate on the aviation sector. The tool must allow for multiple stakeholder agencies to populate the system with daily activity reporting, intelligence and informational data, and key flight information. This data would be triangulated with flight pattern information, and key critical infrastructure data to develop probability scores for potential high-risk flights. These probability scores would then be used as a tool to assist in resource deployment. The probability modeling tool must be developed using the following summary

variables: impact, vulnerability, threat, and intelligence.

The deliverable will be a probability tool with geospatial and event-based display capability that has the capacity to incorporate resource deployment matrices tailored to specific events. The output for this prototype will be a prioritized list of flights contained within the Official Airline Guide (OAG). Such a modeling tool initially will assist in distinguishing the relative risk posed by potential high-risk flights, but over time may be expanded to other transportation modes to assist the Department of Homeland Security (DHS) and other Federal agencies in performing probability modeling and holistic resource planning and deployment based upon the analysis of all available data and identified risk variables.

Configuration:

- The prototype platform will be a standard Windows-based desktop
- The prototype will be compatible with the DHS certification and accreditation process
- The prototype will operate at an unclassified level, but may access and contain law enforcement-sensitive and Homeland Security-sensitive information
- The prototype must be able to access flight information from a database containing a subset of the Official Airline Guide (OAG)
- The prototype will return an answer in less than two hours, preferably faster

Field conditions for use:

A typical office environment.

Users:

- Information Analysis/Infrastructure Protection (IA/IP) and Federal Air Marshall Service (FAMS)
- Counterterrorism agencies government-wide.

Deliverables:

- **Interim Deliverable**
  - High-level software specification which must be approved by the government before further development
- **Final Deliverables**
  - A prototype software application
  - User documentation

Field Testing:

A field test is required, requiring participation by prototype developer. The field test will be operation of the prototype at a DHS component, including 7 cycles over a 7-day period (Monday-Sunday). Key elements to be tested are: speed and ease of operation, accuracy of risk projection. During the test, the prototype will load the data from all required data sources, including representative data from OAG, Critical Infrastructure Database, and special events. In operation, each database will have tens of thousands of records, but probably no more than 20 fields per record. The test will be performed on a subset of this data. Upon contract initiation, the Government will provide applicable data structures.

FINAL

3.1.4.2 ITG2 – Significant Encounters Visual Environment (SIEVE)

Descriptive Title:
Significant Encounters Visual Environment (SIEVE) Prototype

Description & Specification:
The contractor shall develop a real-time port and border encounter monitoring system. This system must incorporate Geographic Information System (GIS) layered data-mapping technologies with established reporting and watch procedures. The system must reach out to other, existing Customs and Border Protection (CBP) and Immigration & Customs Enforcement (ICE) systems for initial reporting on encounters by CBP field operators. The visual interface must facilitate access to a complete collection of information from existing CBP/ICE systems via Office of Intelligence (OINT) analysts' desk terminals. The system must allow for additional analysis to be uploaded by OINT analysts at the headquarters level. All of the information associated with a single encounter must be presented in a standardized report format. The system must be intelligent enough to recognize similarities between encounters and produce warning indicators when patterns emerge. These patterns must then be used to indicate future possible encounters based on historical trends. The contractor shall bid an option to maintain and enhance the software for one (1) additional year.

Significant Features:

Performance

- GIS Analytical Interface
  The prototype must graphically display significant encounter reporting on maps such as the world, U.S., regions of the U.S., border patrol sectors, etc. The maps will be pre-loaded with existing CBP/ICE facilities as points of reference. These facilities will include:

  - CBP Ports of Entry (POEs)
  - CBP Pre-clearance Offices
  - Container Security Initiative (CSI) Offices
  - The Air and Marine Operations Center (AMOC)
  - Border Patrol Sector Offices, Stations and Sub-stations
  - ICE Detention Facilities
  - ICE Resident Agent in Charge (RAIC) Offices
  - ICE Special Agent in Charge (SAIC) Offices

  Significant encounter spot reports will be uploaded automatically from the CBP Commissioner's Situation Room into the GIS interface. Encounters will be displayed as color-coded icons. Each different color will represent a different type of event. The events reported will include terrorism-related activities, attempted human smuggling incidents, radiation detections which merit an official Department of Homeland Security/Department of Energy (DHS/DOE) response, officer safety issues, possible surveillance, narcotics, currency, merchandise

FINAL

seizures of a certain scale, foreign military or law enforcement incursions, and absconders.

The uploaded spot report and color-coded GIS display will constitute the first layer of information about a significant encounter. This first layer will be available as soon as they are reported from the field.

- Automated Retrieval of Disseminated Reporting

The second layer of information consists of standard reports filed by field elements within CBP. These reports are disseminated through the Treasury Enforcement Communications System (TECS). The SIEVE system must have the ability to reach out to TECS in order to retrieve the information contained in these reports. Retrieved reports must be appended to the initial spot report to complete the second layer of information. This second layer must be able to reach out to the following government-owned databases with the capability to add other databases in the future: Primary and Secondary Inspection records, Incident Logs, and ENFORCE database entries. These records must be combined with the National Targeting Center Log detailing each encounter. All of these records must be added to the encounter report.

Upload Feature for Finished/Disseminated Intelligence from External Sources

The third level of information must consist of classified information that individual CBP OINT analysts will add after conducting further research. After initial examination of each encounter is complete, CBP OINT analysts will add any classified material up to and including the SECRET level to each encounter report. These reports must then be archived on the system for future research. The system must be compatible with existing gateguard technologies. The contractor must have access to some personnel cleared to the TS/SCI level to support testing and troubleshooting.

Report Generation Capability

At the request of an analyst, the SIEVE system must generate a complete encounter report, which must include all three levels of information mentioned above. In addition, the SIEVE system must automatically display significant encounters recorded within the past 24 hours on the GIS interface. An analyst shall be able to navigate this GIS interface and retrieve via a “point-and-click” system complete and incomplete encounter reports as they appear. Some reports will be time-tagged and some will not; the system should be capable of dealing with both. The government will give preference to proposals that provide for both capabilities.

Intelligent Recognition of Similarities

FINAL

The SIEVE system must maintain a searchable database of essential elements of information for each encounter. The system must have a robust search capability against a variety of variables, both from structured and unstructured queries. The detailed description of the data structures and the connections of this system with other Homeland Security entities will be protected at the Sensitive Security Information (SSI) level.

- Configuration

The SIEVE system will be hosted on a government-provided Local Area Network (LAN) with four (4) access terminals. The system must not connect to sources outside of the CBP Intranet. This will allow the system to access CBP proprietary systems, such as TECS, but not the Internet. Each of the terminals must allow for research into and updating of reports. Only the terminal located in the OINT Operations Center will allow for the addition of and viewing of classified information.

The desktop systems will need to consist of graphics cards and drivers powerful enough to handle rapid rendering of visual displays via the GIS interface. Because the information contained within the SIEVE prototype reports will be textual (not graphical), the prototype LAN will be able to run off a small central Blade-type server.

Later versions of the prototype may require larger capacity servers with greater processing power, as more data and graphical content is added.

Standards:

The SIEVE system may contain proprietary, personal, For Official Use Only, or Law Enforcement Sensitive information. The system must adhere to the restrictions contained within the Privacy Act governing the disclosure of personal or proprietary information. In addition, final reports will likely contain sensitive or classified information. For this reason, the system must adhere to restrictions on the use and dissemination of classified information as per Department of Homeland Security regulations, and other guidelines as appropriate.

Field Conditions for Use:

The prototype will be operated in a typical office environment.

Users:

- CBP Headquarters Office of Intelligence
- Other DHS entities

Deliverables:

Deliverable(s) and Key Decision Points

FINAL

Deliverables & Key Decision Points	Month After Contract (MAC)
1. Kick-Off Meeting	1.0 MAC
2. Preliminary Design Review (PDR)	2.0 MAC
3. Software Documentation (draft): System/Subsystem Design Description, Interface Design Description Software Installation Plan, & Software Transition Plan	3.0 MAC
4. Conduct Critical Design Review (CDR)	3.5 MAC
5. Interim Progress Review (IPR)	6.0 MAC
6. Interim Progress Review (IPR)	9.0 MAC
7. Interim Progress Review (IPR)	12.0 MAC
8. Test Readiness Review (TRR)	14.0 MAC
9. Internal tests at contractor facility	14.5 MAC
10. Updated Software, System/Subsystem, & Interface Documents	15.0 MAC
11. Draft Software User Manual and Software Test Plan & Description	15.0 MAC
12. Operational tests at Government facility	15.0 MAC
13. Test Results	17.5 MAC
14. Final delivery of software and final documentation	18.0 MAC

Each performer will submit monthly technical and financial reports Program Progress Report (DID# DI- MGMT-80555) and Funds and Man-Hour Expenditure Report (DID# DI-FNCL-80488)

Within eighteen (18) months of the start of the development cycle, a prototype Local Area Network (LAN) hosting the SIEVE system should be deployed at CBP Headquarters. Training should take place within one week of the system being used by OINT analysts. The system will consist of a LAN with four (4) terminals, able to be accessed from the OINT Operations Center, The Office of Intelligence, the Border Patrol Office of Intelligence, and the Commissioner's Situation Room (with restrictions on viewing classified information in the latter two cases). Within eighteen (18) months, all of the desired specifications detailed above will be provided in the initial SIEVE prototype.

Field Testing:

The contractor shall use an iterative development process. The contractor shall perform most of the software development at their own location. The contractor shall support beta testing by the government at a government location.
For the initial prototype, field-testing will take the form of operating the SIEVE system within CBP OINT at the headquarters level.

Upon the completion of the field testing, the prototype SIEVE system will be deployed at four locations within CBP Headquarters: the CBP Office of Intelligence, the CBP Intelligence Center, the Border Patrol Office of Intelligence, and the Commissioner's Situation Room. The initial prototype will gather any and all reportable information concerning the northeastern section of the United States – Canada border. All air land and sea Ports of Entry in the Northeast region will fall within the scope of SIEVE

FINAL

collection requirements. Border Patrol reporting from the Swanton, Houlton, and Buffalo sectors will be included.

3.1.4.3 ITG3 – Modeling the Complex Urban Environment (MCUE)

Descriptive Title:

Mapping Threats to Vulnerabilities to Emergency Preparedness and Response within a Complex Urban Environment

Description & Specifications:

The contractor shall develop, test, and field a near real-time system that maps group and tactic specific threats to specific vulnerabilities and to emergency preparedness and response within a complex urban environment. The system must incorporate the following three features: rapid pattern discovery, rapid pattern projection, and hypothesis testing and visualization. The system must support the analysis of disparate geo-coded information from Governmental and non-Governmental sources, accepting standard geo-spatial input formats and yielding commercial standard output formats. The system must provide a visual display of results at the single and multiple data layers.

Significant Features:

Performance

- Pattern Discovery

  Pattern discovery technologies shall support pattern assessment of foreign and domestic threats.
  - Pattern discovery techniques shall be applied to the data classes specified herein and available within the current defined scenario.
  - Pattern discovery shall be completed in less than 3 hours once data are formatted.
  - Once a pattern is established, its internal parameters shall be editable in near real-time to support hypothesis testing.

- Pattern Projection

  Pattern projection technologies shall support automated mapping of threats to vulnerabilities in designated areas of concern within the U.S. and rapid pattern projection on to a designated U.S urban environment
  - Mapping threats to vulnerabilities shall include the U.S. equivalent data classes specified herein and available within the current scenario.

FINAL

- Mapping threats to vulnerabilities shall be completed in less than 3 hours once data are formatted.
- Once a pattern is projected, its internal parameters shall be editable in near real-time to support hypothesis testing.

- Decision support technologies

  Decision support technologies shall include but not be limited to visualization, situational awareness, emergency preparedness, and emergency response.
  - Visualization within a 2-Dimentional (2D) "Command and Control" view.
  - Planning technologies to support hypothesis testing and contingency planning and execution.
  - Situational awareness shall include but not be limited to identification of intended use for commercial property; product, capacity, and storage limits of production facilities such as chemical plants, etc; structural data such as buildings height, ingress/egress, etc.).
  - Emergency preparedness shall include real-time identification of fixed and mobile emergency service, such as but not limited to medical (hospital, clinics, ambulance services, etc), fire and rescue, HAZMAT, etc.
  - Emergency response shall include dynamic route planning, near-real-time capacity and availability of emergency services, etc.

- Data requirements

  Data sources and classes: Data sources for this prototype shall include but not be limited to geo-spatial data from the National Geospatial Intelligence Agency (NGA), Homeland Infrastructure Foundation-Level Database (HIFLD) Working Group, local Governments, and a wide variety of commercial data vendors. Data classes shall include the following: Government, Civilian, Transportation, Public Health, Emergency Services, Defense Industrial Base, Information and Telecommunications, Energy, Banking and Finance, Insurance, Chemical Industry, and Demographics.
  - **Input requirements:** File Driven: ESRI Shapefiles, MrSID Raster, GeoTIFF; Database Driven: ESRI ArcSDE/Oracle Spatial/PostgreSQL; Standards Driven: Federal Geographic Data Committee (FGDC)/ Open GIS Consortium (OGC) Compliant Spatial Formats
  - **Output requirements:** File Driven: ESRI Shapefiles, ESRI Grid, GeoTIFF; Database Driven: ESRI ArcSDE/Oracle Spatial

Training Requirements:

Training will be simultaneous to operational testing and shall include Government review and approval of a contractor developed operator's manual.

Field Conditions for Use:

The operational environment shall be consistent with current analytical environment currently used by Office of Information Analysis (OIA) and Border Transportation Security (BTS).

FINAL

Users:

- OIA and BTS
- Law Enforcement

Deliverable(s) and Key Decision Points:

1.	Kick-Off Meeting	1.0 MAC
2.	Preliminary Design Review (PDR)	2.0 MAC
3.	Software Documentation (draft): System/Subsystem Design Description, Interface Design Description Software Installation Plan, & Software Transition Plan	3.0 MAC 3.5 MAC
4.	Conduct Critical Design Review (CDR)	6.0 MAC
5.	Interim Progress Review (IPR)	9.0 MAC
6.	Interim Progress Review (IPR)	12.0 MAC
7.	Interim Progress Review (IPR)	14.0 MAC
8.	Test Readiness Review (TRR)	14.5 MAC
9.	Internal tests at contractor facility	15.0 MAC
10.	Updated Software, System/Subsystem, & Interface Documents	15.0 MAC
11.	Draft Software User Manual and Software Test Plan & Description	15.0 MAC
12.	Operational tests at Government facility	17.5 MAC
13.	Test Results	18.0 MAC
14.	Final delivery of software and final documentation	

Month after Contract (MAC)

Each performer will submit monthly technical and financial reports Program Progress Report (DID# DI- MGMT-80555) and Funds and Man-Hour Expenditure Report (DID# DI-FNCL-80488)

Operational Testing:

Operational testing will include three months at OIA's Living Laboratory with active support from the developer. Testing will include operational scenarios as defined by OIA and BTS.

- Derived models shall be validated in an experimentally blind study of historical information.
- Projected and decision support models shall be validated by a multi-discipline subject matter expert panel including, but not limited to, terrorism experts, behavioral scientists, urban planners, security experts, etc.
- Automated model development and testing platform shall be tested against manually derived models for accuracy and speed.

3.1.5 Information Technology – Sharing (ITS) Topics:

3.1.5.1 ITS1 – Geospatial Modeling of Homeland Security Capabilities

Descriptive Title:
Geospatial Modeling of Homeland Security Capabilities

Description & Specifications:

Homeland Security Presidential Directive (HSPD)-8[16] requires an integrated national approach to preparedness because incidents of national significance require a coordinated response employing resources from all levels of government. For this reason, it is important to develop national consensus in defining needed capabilities and setting general target levels for those capabilities against the National Planning Scenarios. No single jurisdiction or agency would be expected to have sufficient levels of every capability needed for a major event. Requirements that exceed a jurisdiction's or agency's capabilities would be secured through mutual aid, State resources, assistance compacts, or Federal support.

Capability definitions are general and expressed in broad operational terms and essential characteristics. The target capabilities are combinations of resources that provide the means to achieve a measurable outcome resulting from performance of one or more critical tasks, under specified conditions and performance standards. A capability may be delivered with any combination of properly planned, organized, equipped, trained, and exercised personnel that achieve the expected outcome. Version 1.1 of the Target Capabilities List (TCL)[17] identifies 36 target capabilities, such as: Mass Care, Medical Supplies Management and Distribution, Search and Rescue, Medical Surge, Interoperable Communications.

Requests to the Department of Homeland Security (DHS) and other agencies for preparedness assistance will ultimately be expressed as capability needs with clearly defined requirements, namely:

- why a capability is needed to be improved;
- how the capability will be used;
- what function the capability will perform;
- who will need the capability;
- when the capability will be available;
- what key performance and other attributes comprise the capability;
- how the capability will be supported;
- what skills will be required;
- how we train responders; and,
- how much the capability will cost

Homeland security planners need to be able to analyze the location and capacity of resources for each capability to effectively respond to these requests.

Federal, state, and local governments utilize geographic information systems to meet a variety of needs. However, homeland security capability analysis models (for the TCL) are lacking. This project seeks to develop and test capability models in a geospatial system to allow Homeland Security planners to visualize preparedness information and perform quantitative analysis (such as coverage area, deployment time, and mutual aid dependencies).

---

16 *See HSPD-8 (http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html)*

17 *See http://www.ojp.usdoj.gov/odp/docs/TCL1_1.pdf*

FINAL

The contractor shall work with Subject Matter Experts (SMEs) at DHS and government-furnished information to develop a software package incorporating Commercial Off the Shelf (COTS)/ Government Off the Shelf (GOTS) software to the greatest extent possible. This development is expected to be iterative with feedback from customers. The final package must have the following characteristics:

Performance:

REQUIRED

- Ability to geospatially model all homeland security capabilities from the Target Capabilities List (TCL)
  - DHS will prioritize which capabilities will be selected for modeling at time of award
  - There will be at least 7 capabilities included
- Flexible visualization of regional capabilities including multiple views such as drill down, toggling between attributes, etc.
- Ability to perform quantitative analysis of components that contribute to capabilities, such as: response time, training levels, coverage area
- Ability to combine (aggregate and weight) components into a single measure of capability (for example, mass care includes multiple measures of capability such as shelter capacity, feeding capacity, shelter management, etc.)
- Dynamic reporting such as the ability to create tabular reports and/or outputs/files on capabilities and regions.
- English language-based

DESIRED

- Ability to localize to foreign languages at a future date

- *Configuration:*
  - Personal Computer (PC) Windows-based
  - Data from readily available government sources, supplemented with local data as provided by DHS

- *Cost considerations:*
  - Prototype should be cost effective, utilizing existing geospatial software
  - Preference will be given to prototypes that have minimal COTS licensing costs
  - DHS requires a fully-paid-up, royalty-free license to use at the Federal level and to distribute to other governmental entities, domestic and foreign

What are the field conditions for use?

The prototype should be functional in a typical office environment

Users:

- Office of State and Local Government Coordination and Preparedness/ Office for Domestic Preparedness
- Federal, State, Regional, Local, and Tribal Homeland Security planners

What is (are) the deliverable(s)?

FINAL

- **Interim Deliverables**
  - Design review (government will give feedback based on design review)
  - Test plan
- **Final Deliverables**
  - Capability models (for the capabilities specified by DHS)
  - Tested and validated software package based on DHS-supplied data
  - User documentation

Field Testing:

Field tests of capability models with Homeland Security planners as they are developed. Use of practical data sets, intuitive visualization, and quantitative reporting are key parameters of success.

3.1.5.2 ITS2 – Resource Awareness Data Portal

Descriptive Title:

Resource Awareness Data Portal

Description & Specifications:

Rapid, effective response to a disaster requires timely access to relevant resource data so that decision makers at all levels of government involved in managing the response operation can make informed decisions. These critical decisions direct the deployment and use of limited but shared resources to protect the public and critical assets as well as mitigate the effects of the disaster.

Community, regional, state and federal agencies maintain and operate disparate resource databases that support the daily functions performed by the individual agencies. The data stored in the individual databases can be required to mount an effective multi-agency, multi-jurisdictional response to emergencies under existing mutual aid agreements and statutory authorities. What is missing is a standard "universal" mechanism that merges that resource data stored in the differently formatted and configured databases into a single, virtual, federated, networked system that allows both sharing and use of data to support unified and integrated decision making processes among the participating agencies, regardless of agency location or level of government.

The contractor shall develop an operational emergency management / emergency response data fusion solution based on and built with commercial-off-the-shelf and government-off-the-shelf applications that creates a shared virtual data repository of resource data in a "just in time" manner. Data from legacy data centers as well as new data arising from the on-going disaster response will be fused to support specific operational requirements. The virtual data solution must provide a graphical user interface that enables authorities to quickly set or change:

- Role-based security levels;
- User access privileges;
- Identify data to be shared; and
- Produce reports and analyses using an integrated suite of tools.

Interaction with the virtual data repository must be through a standard Internet browser

interface employing standards-compliant extensible languages and protocols. The contractor shall provide a secure, virtual prototype for the sharing of resource information by authorized users to support prevention of, planning for, response to, and recovery from acts of terrorism and other "all hazards" events. The initial solution version (prototype) will be deployed to one or more regional sites for test and validation.

Performance:

- The portal must be browser-based and provide controlled, secure access to a variety of resource data located in different, unrelated databases [e.g., Resource Ordering and Status System (ROSS)] operated by the participating response agencies.
- The portal must be compatible with the local, state, and federal data sources used in the field testing of the prototype.
- The portal must be designed to be National Incident Management System (NIMS)-compliant and to meet relevant NIMS standards
- The portal must provide secure and unsecured access capability through a browser interface that can deliver just-in-time resource data.
- The portal must be installable, configurable and maintainable by current user personnel. It cannot require contractor or federal government support beyond that typically provided by vender installation and “help desk” staff.
- The portal must be capable of running on existing user computer hardware and Microsoft Windows over high speed wired networks, wireless access and low bandwidth dial-up.
- The portal must provide aggregate and filtered views (e.g., by resource type or location).
- The portal should provide output that can be input to a Geographic Information System (GIS) visualization system.

o **Configuration**

- A distributed, federated approach to data sharing that enables Federal, State and Local agencies to control and maintain their own data systems while simultaneously deciding what resource data to share through the data portal and with whom to share the data using access control and authorization technology.
- The data portal should be built using commercial-off-the-shelf and government-off-the-shelf software and conform as required to existing and emerging emergency management information technology standards such as the Common Alerting Protocol (CAP) and the emerging Emergency Data Exchange Language (EDXL) protocol under development by the Organization for the Advancement of Structured Information Standards (OASIS) group, the National Information Exchange Model (NIEM), the Global Justice Extensible Markup Language (XML) data model (GJXDM), and the emerging Unified Incident Command and Decision Support (UICDS) architecture.
- Business rules and governance protocols that enable users to identify data to be shared.

o **Standards:** Contractor must coordinate with the Office of Interoperability and Compatibility, the Science and Technology Standards Portfolio, and the Office of State

FINAL

and Local Government Coordination and Preparedness to ensure compliance with latest Homeland Security directives regarding interoperability and compatibility of public safety systems and compliance with the implementation of the NIMS.

- **Cost Considerations:** The Department of Homeland Security (DHS) requires a fully-paid-up, royalty-free license to use at the Federal level and to distribute to other governmental entities, domestic and foreign, any custom database adapters or wrappers that are developed to interface with legacy systems.

- **Training requirements** Vendor will develop browser-based training materials for system administrators and users to be used in field testing.

Field Conditions for Use:

The prototype should be operational in deployed field environments where a laptop personal computer (PC) is used.

Users:

- Office of State and Local Government Coordination and Preparedness / Office of Domestic Preparedness.
- Public safety regions throughout the U.S.

Deliverables:

- Interim
  - Design review
  - Lab test plan
- Final
  - Resource awareness data portal as described above
  - Browser-based training

Field Testing:

The government will conduct field testing in one Urban Area Security Initiative (UASI) location. The vendor will support the field testing.

3.1.5.3 ITS3 – Tactical Information Sharing System (TISS) Image Analysis Capability

Descriptive Title:

Tactical Information Sharing System (TISS) Image Analysis Capability

The contractor shall provide application software that performs facial image comparisons for the purpose of identifying possible criminals and terrorists. Some of the images are captured from low resolution devices.

The prototype will generate full frontal facial images from partials. The prototype will perform digital image comparisons.

Description & Specifications:

FINAL

- The Tactical Information Sharing System (TISS) captures Federal Air Marshall Service (FAMS) observations of suspicious activity in the aviation domain. TISS enables FAMs in the field to report the surveillance of suspicious behavior and activity, instantly into a database for analysis, and provides information sources for examining long-term trends and patterns.

  Federal Air Marshall Service (FAMS) image analysis capability shall define an automated method of manipulating an image of a person, based up physical characteristics, in order to make the image compatible with biometric algorithms used with Facial Recognition or image comparisons.

  FAMS image analysis capability shall have the abilities to connect to the FAMS TISS. The prototype shall have the abilities to mensurate and manipulate images to a level in which the image can be used for electronic image comparisons. FAM analysts in the Tactical Information Branch (TIB) will perform these comparisons on desktop systems.

  - Performance: What *must* the prototype actually do?

    The operational objectives of image analysis application are as follows:
    It must:

    1. Have the ability to create a face-forward, "line-up" style image from a submitted profile or angled image which will be stored and maintained in TISS with associated meta-data
    2. Have the ability to re-create missing sections of an image based upon key measurements of the available image
    3. The prototype will produce a list of images from the TISS database that most closely match the generated image
    4. Return rates are specified by the user
    5. Comparisons will be completed in near real time
    6. Connect to Tactical Information Sharing System (TISS) database
    7. Allow the user to compare standard images formats (e.g. Joint Photographic Experts Group (JPEG), Windows Metafile Format (WMF), BITMAP, Graphic Interchange Format (GIF) , Tagged Image File Format (TIFF), etc...)
    8. Operate for both color and black and white images
    9. The application will produce a ranked list of images based on match rate
    10. Have the ability to send the results and the altered image to a printer and/or to a file
    11. Must operate under low light conditions, but not be adversely affected by a sudden burst of light

  - Configuration:
    - The prototype will run on a standard Microsoft (MS) Windows Desktop platform (2000 or XP platform)

  - Training requirements:

    1. The contractor shall provide written material describing the prototype and its operations.
    2. The contractor shall provide training during field trials sufficient to allow the operators to safely and effectively operate the system.

FINAL

What are the field conditions for use?

In a typical office environment.

Users:

- Department of Homeland Security (DHS) - Immigration and Customs Enforcement (ICE)
- Federal Air Marshal Service

Interim Deliverables:

(1) Preliminary design review (estimated within 2 months of program start); the design must be accepted by the government before prototype development.
(2) Critical design review; the design must be accepted by the government before prototype fabrication.
(3) Test plan for the Preliminary Field Test
(4) Preliminary Field Test report

Final Deliverables:

(1) Final Report, including prototype description and operations.
(2) Operational prototype
(3) Training, user manuals

Testing:

Operational Field Test:

(1) The contractor shall develop test criteria incorporating guidance from the FAMS Subject Matter Experts (SMEs) to assist prescribing necessary parameters. The contractor shall provide training for up to 4 users who will operate the prototype during the test. The operators should be trained to a level that they can train additional personnel. The government will conduct a field test at a single location with the technical assistance of the contractor. The test is not expected to exceed two weeks. The government will provide beta test data for the tests. The contractor shall capture test results in the Preliminary Field Test report including first-hand constructive feedback from the end user and any shortfalls in the prototype's operations.
(2) Government will provide sample images and data structures for TISS.

Key Elements to Consider for Preliminary Field Testing:

The key elements shall include the abilities to map facial structures and objects from images, by manipulating known measurements of the image, and compare these images to other available image databases. Primary features will include the successful execution of:

1. Image re-generation
2. Image comparisons / matches
3. Results ranking

- How many prototypes are required for field-testing? One prototype with up to 4 group users.

FINAL

- Is participation by the prototype developer desired? Yes.

3.1.6 Electronics and Hardware (EH) Topics:

3.1.6.1 EH1 – Advanced 3-D Locator System

Descriptive Title:

Advanced 3-Dimentional (3D) Locator System

Description & Specifications:

There is a need to be able to accurately locate and track incident responders in situations such as: inside of threatened buildings, collapsed buildings, and subterranean facilities or underground. Accurate location and tracking is necessary in order to allow emergency managers, including fire chiefs and other incident commanders, to rapidly and effectively deploy and re-deploy their forces or understand and respond to the consequences of potential threats to their forces.

- *Performance*:

  REQUIRED

  - Locator must not impede the normal activities of incident responders.
    - Locator must be compatible with existing equipment and procedures
  - Locator must send information including location-related information and unique identifier.
  - Locator must have an incident life of 2 hours or longer (4 hours desired).
  - Locator must include a distress button and indicator of non-movement.
  - Locator must wirelessly transmit inside or outside of structures and through rubble to an off-site incident command post, on-site incident command posts, emergency responders, and/or other authorized parties including within teams of responders.
  - Locator must be self-initializing, self-calibrating, self-adjusting and must have self-diagnostic capabilities to ensure speed and reliability.
  - Locator must be able to function in the extreme heat and cold typical of the operational environments encountered by emergency responders.
  - Locator must be resistant to potentially damaging electrical charge, protected from potentially dangerous gases, impact resistant, and waterproof.
  - Locator must operate outside all buildings and inside of almost all buildings, no matter their structural state and environmental conditions.
  - Primary incident command posts should be able to monitor the status of the locator and its host from a radial distance from 30 meters to 100 meters (per relay).
  - Locator must be able to specify the location of its host in three dimensions within 6 meters (3 meters desired).
  - If ancillary antennas are used by the relays between the locators and the base station, highly accurate or fixed locations for the relays must not be required.
  - The base station is a combination of additional communications equipment and the laptop/portable computer and required software.

FINAL

- The base station must be designed so that the laptop can be any current ruggedized Microsoft Windows® laptop/portable computer.
- The base station software must be able to display location and identification of personnel.
- The base station must be able to display general-to-specific information (the ability to drill down from an overall scene to a specific individual) about an operation/incident and its emergency responder participants.
- The base station software must be able to link the unique identifier of the locator to a specific individual.
- The base station software must be able to record activity for replay.
- The base station must include visualization tools that :
    - Allow incident commanders and site personnel to easily interpret incoming displayed information.
    - Display the location of an emergency responder in easy to understand coordinates. (One form of display must be a wire-frame like view of the building structure with the position of each responder indicated. The wire-frame view must include a scale showing grid spaces of approximately 10 feet in every direction.)
    - Allow the user to identify, group, and categorize responders as desired
- The base station display update interval must be adjustable to as little as five seconds.
- The user of the base station must be able to change the screen display according to the scope of the situation.
- The base station unit must be resistant to water, heat, and other normal environmental stresses encountered by emergency responders.
- Optionally, the coordinates returned by the locator can be input to a Geographic Information System (GIS) system (including a building map or equivalent for underground structures).

- *Cost Considerations*:
    - Final product should be cost-effective to facilitate widespread adoption by the responder community

Field Conditions for Use:

The prototype should provide timely operational support for all-discipline, all-hazards scenarios in a broad range of environmental conditions and terrain.

Users:

- Department of Homeland Security (DHS) Emergency Preparedness and Response Portfolio
- Federal, State, Local and Tribal incident responders and managers
- DHS / Emergency Preparedness / Federal Emergency Management Agency (FEMA)
- All lead and supporting Federal agencies of the National Response Plan
- Law Enforcement agencies
- Fire Departments

Deliverables:

- **Interim Deliverables**

FINAL

- Design Review
- Laboratory Test Plan

- **Final Deliverables**
  - Prototype Design Document and Final Report
  - Prototype (includes 2 base stations and 50 field-testable locators and all other relays as necessary)
  - Successful field exercises, demonstrations, and training

Field Testing:

Development of the prototype should include testing of individual components, the integrated system, and field exercises. Successful integration, ease-of-use, and value-added as determined by responders and incident commanders are key parameters of success. Government will design the field tests.

3.1.6.2 EH2 – Extreme Wide Field-of-View IR/NV Capability

Descriptive Title:

Extreme wide field-of-view infrared/night vision (IR/NV) capability for use during high-speed night intercepts for marine and land missions

The contractor shall provide a marine/land-based prototype that provides vessel and vehicle operators a wide-peripheral awareness stereo-optic vision (for depth perception), low moment arm, night-vision capable system. The prototype must be capable of surviving high accelerations/decelerations and allow the operator to view both the horizon and internal vessel/vehicle controls.

The focus of this device is to increase peripheral vision and to reduce neck and head strain caused by existing infrared/night-vision systems.

Description & Specifications:

Nighttime conditions, during less than overt intercepts, and adverse weather, are extremely taxing on coxswains. Existing wearable infrared/night vision systems are extremely limited in field of view (FOV) and field of regard (FOR) affecting the coxswain's depth perception. The limited FOV requires constant motion in order to take in objects in the water and to read and maintain awareness of multiple boat parameters (revolutions per minute, etc.) affecting stable images and rapid awareness of dangerous conditions. The environment (even in good weather) often results in head and neck trauma from the moment arm produced by existing monocular and binocular systems.

The prototype shall meet the following criteria:

- Minimum of 125 degrees (threshold is 125 degrees; 150 degrees desired) in azimuth x 50 degrees in elevation
- Must meet or exceed existing Generation III IR/NV systems for reactivity to changing light conditions
- Must mate with ballistic and impact helmet systems presently used by U.S. Coast Guard (USCG) coxswains

FINAL

- Must operate through windshields or direct exposure to the environment
- Must survive momentary and frequent submersion in saltwater
- Self-contained (sealed) power systems
- Should be capable of using standard batteries in an emergency
- Must provide a low power warning indicator
- The power source(s) should be rechargeable
- Highly reliable with Mean Time Between Failure (MTBF) > 1000 hours with a Mean Time To Repair (MTTR)< 8 hours
- Resistant to particulate depositing that impacts resolution
- Performance does not degrade in 100% condensing atmospheres
- Very lightweight with high degrees of mobility, acuity, and minimal strain on the user
- If system fails, view screen shall revert to full clear view

Standards:

- National Electrical Manufacturers Association (NEMA) standards for marine applications
- Shock resistant to American National Standards Institute (ANSI) Standard for impact helmets

Cost Considerations:

- Critical components must be line replaceable units
- The contractor shall give preference to Commercial Off the Shelf (COTS) equipment
- Target production cost shall not exceed $10,000 per system

Training Requirements:

- No classroom instruction required

Field Conditions:

- Sea State 3
- Desert sandstorm conditions
- 100% condensing humidity conditions
- Salt (seawater) spray
- Ideally operates between -20 degrees Fahrenheit and 120 degrees Fahrenheit

Users:

- U.S. Coast Guard
- Customs and Border Protection (CBP)
- Immigration and Customs Enforcement (ICE)

Deliverable(s):

Interim Deliverables:

- Design specifications
- Critical Design Review
- Test Plan

FINAL

Final Deliverables[18]:

- Two fully functional prototypes available for operational testing
- Up to 6 prototypes per each Department of Homeland Security (DHS) potential customer to field-test in different scenarios; must include any mounting/mating hardware for both ballistic and impact helmets
- During test and evaluation, technical and maintenance support shall be available to perform repairs 24 hours/day.
- User manual

Field Testing[19]:

- **Key elements to be tested:**
  - Effects on neck and head strain under operational conditions.
  - Technical performance including validation of field of view, improvements to field of regard, acuity under severe conditions, image stability during positive and negative accelerations, etc.
  - Operational evaluation to determine impact to other systems and potential egress effects.

3.1.6.3 EH3 – Improved Heartbeat Detector System Prototype

Descriptive Title:
Improved Heartbeat Detector System Prototype

The contractor shall deliver a Heartbeat detector prototype utilized for finding concealed passengers or detect motion in conveyances and cargo containers, using several vibration sensors and analysis software with a user interface subsystem.

The emphasis shall be focused on increased deployment and detection speed over currently available Commercial Off the Shelf (COTS) equipment.

Descriptions and Specifications:
Heartbeat detector systems are utilized for finding concealed passengers in conveyances and cargo containers, using several vibration sensors and analysis software with a user interface subsystem. An improved prototype is required, which will enable operations under a wider range of conditions than current available models.

Target specifications include:
The detector prototype shall detect the heartbeat(s) (or subsequent motion) of any live human occupant(s) in conveyances and containers. Conveyances will be stopped and have engines shut

---

18 *S&T Clarification: Two fully-functional prototypes should be available for operational testing, in addition to 6 prototypes for field testing for each of the DHS customers listed. (U.S. Coast Guard, Customs and Border Patrol, and Immigration and Customs Enforcement). This totals to 20 prototypes to be delivered, 2 for operational testing and 18 for field testing, including any mounting/mating hardware for both ballistic and impact helmets.*

19 *S&T Clarification: The Government intends to perform field testing (either directly or via third-party) on delivered prototypes. Offerors should expect to provide 24 hour technical and maintenance support for the delivered prototypes through the testing period, which is not expected to exceed 3 months.*

off during inspection. The detector prototype shall operate with a wide range of conveyances and container types, to include:

- Passenger Cars
- Trucks
- Tractor-Trailers
- Buses
- Trains
- Airplanes
- Cargo Containers
- Cargo Pallets

The improved heartbeat detector prototype shall be capable of facilitating inspection of a conveyance or container for live human occupants in less than 3 minutes. This includes setup, inspection, and removal of the equipment.

It shall be available in a portable configuration, which must allow initial setup in less than 20 minutes. The portable configuration shall be operable from 120 volts alternating current (VAC)/60 Hertz (Hz), or 12 volts direct current (VDC)/8 Amperes (A) from an automobile accessory power outlet, or an optional rechargeable battery pack with a life of no less than 16 hours. When packed for transport, no component shall weigh more than 50 pounds. All prototype components, to include displays, controls, batteries, sensors, connectors and cables, shall be quickly replaceable by operators in the field. Prototypes must be hermetically sealed.

The improved heartbeat detector prototype shall have the capability to connect to a Customs and Border Protection (CBP) secure network. The prototype will be capable of reporting inspection results, accompanied by operator-entered information including: operator name, license plates, and notes to the CBP network. The prototype shall also be capable of reporting diagnostic information (including sensor waveforms) to assist in maintenance and upgrades. The prototype shall be capable of remote software upgrades using the network connection (specs will be supplied).

1. The objective performance requirement for the customer is for the detector system to produce a false positive rate of no greater than 5% and a false negative rate of no greater than 5% under all the operating conditions specified in this document.

2. Provide a clear positive or negative indicator of concealed humans or human movement detection for 100% of all inspections under every specified condition.

3. The manufacturer shall be International Organization for Standardization (ISO) certified.

Training:
The improved heartbeat detector prototype shall be simple enough that Officers/Agents can be fully trained to operate and maintain it in 6 days or less, excluding network functions.

FINAL

Field Conditions:
The improved heartbeat detector prototype shall reject interference due to high winds, rain, or operations of nearby conveyances. It shall reject this interference when operated on pavement, unpaved/gravel areas, and bridges or overpasses.

The improved heartbeat detector prototype shall operate reliably for extended periods under all weather conditions in which US Customs and Border Protection perform inspections. These conditions range from desert heat to arctic cold, and precipitation including snow and rain. The prototype must include both audio and visual display. The display and operator controls shall be easily operable under all weather conditions including bright sun, and audio alerts shall be audible in all of the specified conditions.

All components of the improved heartbeat detector prototype shall withstand repeated rough handling under typical inspection conditions at ports and checkpoints. Displays, controls, batteries, sensors, connectors and cables shall be rugged and waterproof.

Safety:
The unit must not interfere with officer safety or preclude access to an officer's firearm and holster.

Cost Considerations:
Production target cost shall be no greater than $50K.

Depending on the manufacturer, the costs for Heartbeat Detector prototype range from $35K - $75K. For this prototype with a requirement for one year full parts and labor warranty the expected operations & maintenance (O&M) costs will be zero dollars.

Users:

- Department of Homeland Security

Deliverables:

Interim Deliverables:

(1) Preliminary design review (estimated within 2 months of program start); the design must be accepted by the government before prototype development.
(2) Critical design review; the design must be accepted by the government before prototype fabrication.
(3) Test plan for the Preliminary Field Test
(4) Two Heartbeat detection prototypes
(5) Preliminary Field Test report

Final Deliverables:

(1) Final Report, including prototype description and operations.
(2) Operation and Maintenance Manual.
(3) Training materials.

FINAL

(4) Provide training for up to 6 hours, for two locations, for up to 4 people per location of user training who will operate the prototype during the test. The operators should be trained to a level that they can train additional personnel.

Field Testing[20]:

A field test will be performed on the prototype by a government specified testing authority. The supplier will provide required personnel to respond to test team needs.

The conditions the equipment should be tested under will, at a minimum, include:

1. Low to Medium wind velocities (Wind velocities in increments of 5 miles per hour (MPH) between the range of 5 MPH to 40 MPH)
2. Range of light to heavy rain.
3. Temperature ranges of -20 degrees Fahrenheit - +120 degrees Fahrenheit
4. Nearby ignition of a large diesel engine.
5. Passing nearby conveyance traffic.
6. Repeated rough handling.
7. Bright sun and darkness.

Provide the following for prototype test and evaluation:

- Test plan prepared by supplier in conjunction with a government third party test facility.

- Test report prepared by supplier in conjunction with government test team. The test report will identify results of the prototype tested under third party field testing conditions.

3.1.6.4 EH4 – Advanced Urban Search and Rescue (US&R) Breaching Approach

Descriptive Title:

Advanced Urban Search and Rescue Breaching (US&R) Approach

Description & Specifications:

Background: An advanced breaching (i.e., cutting, coring, burning) and breaking prototype will allow faster and safer extrication of victims from disaster sites. Current methods use standard power tools (i.e., saws, drills, jackhammers) and could take four to six hours for the most difficult materials.

Tasking: The contractor shall develop and demonstrate one or more technologies and techniques (approaches) that when combined will produce rapid breaching and breaking. Only approaches that are amenable to final deployment in man-portable configurations will be acceptable. However, during this project, the contractor only needs to demonstrate

[20] *S&T Clarification: The offeror should expect to provide technical and maintenance support for field testing at a government-specified testing authority for a period not expected to exceed 3 months, in addition to the pre- and post- testing tasks specified.*

the effectiveness of the approach. The contractor shall define a test plan including specification of materials and configurations.

- *Performance*:

  REQUIRED During this Project

  - The approach must perform the breaching and breaking functions an order of magnitude faster than present breaching systems (required 30 minutes or less).
  - The approach must function without destabilizing the structure any more than present systems.
  - The approach must function without injuring victims or operators.
  - The approach must penetrate most building materials (e.g., concrete, rebar).
  - The approach must be designed so that level of training and skill required to operate the tool in its final configuration must be commensurate with current breaching systems.

  DESIRED End State Configuration

  - Be operable by a single emergency responder in a restricted space.
  - Cutting capability with depth control.
  - Perform multiple functions (i.e., cutting, breaking, sawing) in one modular structure.
  - Long life, self-contained mode and externally-powered / supplied mode
  - Final production configuration should be portable and lightweight so that it and all necessary support equipment can be carried (including up stairs) to a scene by two responders.
  - Packaged in a "go" pack that can be carried in a small vehicle.
  - Durable.
  - Functional in any urban environment.
  - Include all unique safety equipment required for use.
  - Be affordable by urban search and rescue teams.

Field Conditions for Use:

This tool(s) will be used in search and rescue operations in disaster or emergency situations. The tool must be functional in any environment; specific scenarios include man-caused (e.g., bombings, terrorism) or natural (e.g., hurricanes, tornadoes, earthquakes) creating collapsed, damaged, and unstable structures.

Users:

- Federal Emergency Management Agency (FEMA) Urban Search & Rescue (US&R)
- Emergency Medical Services (EMS)
- Law enforcement agencies
- State and Local Urban Search and Rescue (US&R) Teams
- Heavy Rescue Teams

Deliverables:

- Interim
  - Test Plan (government will review)
- Final
  - Demonstration of technology and techniques [One (1) Unit]

FINAL

- Test Results
- Final Report

Field Testing:

The only testing required is that defined by the contractor and approved by the government to be performed in the contractor's facility.

Reference:

Urban Search and Rescue Technology Needs Report, US Department of Justice, Office of Justice Programs, National Institute of Justice, and Department of Homeland Security FEMA June 2004
(http://www.ncjrs.org/pdffiles1/nij/grants/207771.pdf)

3.1.7 Cyber Security (CS) Topics:

3.1.7.1 CS1 - BOTNET

Descriptive Title:
BOTNET Detection and Mitigation Tool

The contractor shall develop a tool for identifying bots and botnets. Technologies developed under this topic must perform their functions within legal and ethical boundaries, while considering how the resultant technology can use the "botnet" mindset and work with other systems that might deploy similar technology in order to defeat the botnets and their malicious activities. The contractor shall use an iterative development and testing approach, working closely with the government.

The proposed BOTNET Detection and Mitigation Tool must be able to automatically scan for associated malicious codes on networks and machines, and then recommend solutions to mitigate the attacks. System administrators would control the application of the tool.

The proposed BOTNET Detection and Mitigation Tool must not adversely impact network or system performance and operations.

Background:
One of the rising problems in today's networks is the existence of bots and bot networks. A Bot is a generic term and is used to describe an automated process in the computer world. Search engines use Bots to spider websites. Online games, such as Quake, use Bots as artificial opponents. Bots do not need external support and will relentlessly do their masters bidding until told to stop. The Bots in question are Internet Relay Chat (IRC) Bots and they operate in much the same manner. An IRC Bot is basically an IRC-controlled script that responds to IRC events on its own without user interaction. A botnet is a collection of compromised hosts (infected with one or more types of bots), under (usually) a single command and control channel (typically on an IRC channel), with its major purpose to do malicious action such as distributed denial of service (DDoS), Identity (ID) theft, keyloggers, phishing and spam. The bots normally contain servant code, one or more exploits and one or more attack tools. Most bots are delivered to

machines via a trojan horse program – hidden code from other files, websites, etc. The trojan will also have been coded to make the bot join a certain channel once it has silently connected to the Internet from the compromised machine. If the trojan has infected many computers, then many bots will join the channel. Some channels have been seen with thousands of bots and each one of those bots represents a computer infected with a trojan. A collection of these bots in a channel is a botnet, and even a couple of hundred of them can cause significant damage when used to attack servers and other machines. The command and control (C&C) for these botnet functions is mostly centralized, using one or more IRC servers. The bots and botnets described above are almost always on the machine without the knowledge of the system and/or owner.

Unfortunately, there is **no set way to recognize a bot**. Usually bots are silent until given commands in a channel, but some may 'report for duty' with a word, phrase or even a dot (period). Bots with the capability to sniff the wire or keystrokes are now ubiquitous. They can be found on all networks, to include government and military networks. These bots dutifully report back their findings to the C&C server, and the "botherder" can use this information for a variety of means. Bots have methods of spreading to other systems by exploiting vulnerability on the target system that allows execution of arbitrary code and targeting of unpatched machines. Every popular bot now includes the PSNIFF (or similar) capability. This is a feature in the bot that allows it to spot other bot infections on a host.

Cost considerations:

- The contractor must identify additional licensing costs for any previously developed solutions that are included in the response to this solicitation
- Cost should not be prohibitive for deployment across the Federal government

Training Requirements:
The contractor shall provide system administrators and other technical users training not to exceed one (1) day.

Field Conditions for Use:
The expected operational environment of the prototype in field use would be a program/tool installed on networks.

Users:

- National Cyber Security Division (NCSD)/ United States Computer Emergency Readiness Team (US-CERT)
- All Federal agencies and critical infrastructure owners/operators (tool to be distributed through authorized government channels)

Deliverables[21]:
Development Plan; Draft Tool Architecture; Final Architecture; Prototype; Test Plan; Field Test; Effectiveness Report; Final Tool; Architecture Documentation; User Manual

[21] *S&T Clarification: Offerors should note deliverables are identified as written in a chronological fashion in terms of program execution. For this effort, the prototype should be a fully-functional tool, ready for deployment and testing in a government-sponsored test facility. After testing, an Effectiveness Report will be generated by the offeror, in conjunction with the government testing team. A final tool will be delivered as an iteration of the prototype tool, integrating changes recommended by the government testing team.*

Field Testing[22]:

Key Elements to be Tested:
- Effectiveness in detecting BOTNETS
- Practicality of recommended mitigation solutions

How Many Prototypes Are Required For Field Testing?
One (1)

Is Participation By The Prototype Developer Desired?
Yes

3.1.7.2 CS2 – Exercise Scenario Modeling Tool

Descriptive Title:
Exercise Scenario Modeling Tool

The contractor shall develop a collaborative web-based tool to assist exercise planners in developing cyber security exercise scenarios for use in cyber training incident response teams. The contractor shall use an iterative development and testing approach, working closely with the government. During this effort, the contractor shall develop a tool to meet the following characteristics:

Description & Specifications:
The Exercise Scenario Modeling Tool is an interactive tool that will assist exercise planners in developing cyber security exercise scenarios for use in cyber training incident response teams.

Performance:
The tool will require a set of decision tree and assessment questions to develop and assess scenario parameters. Examples of assessment subject questions should include but not be limited to the following: communication protocols used, size of network, number of nodes and users, dial up/in access, ownership of communications pathways, security policy, and connections to business networks. Department of Homeland Security (DHS) National Cyber Security Division (NCSD) will provide the final list of questions to be incorporated into the tool. The tool will provide a range of exercise scenario options dependent upon cyber incident response procedures and network parameters.

Configuration:
This tool will be a collaborative web-based interactive program. The server hosting input data will reside in DHS/ Information Analysis/Infrastructure Protection (IAIP). Tool must allow for interrupted work sessions with the ability to preserve entry data. All stored data will be protected for confidentiality and integrity.

[22] *S&T Clarification: Testing will be performed by the government on a government-provided operational network and/or testbed. Offeror should provide separate costed task to provide support for consulting and technical assistance reachback during this government test period, not to exceed one month.*

Standards:
The tool must utilize a graphical user interface. User access and authentication must meet Federal standards.

Cost Considerations:
- The contractor must identify additional licensing costs for any previously developed solutions that are included in the response to this solicitation.
- The contractor shall provide direct support to exercise planners for the duration of the first exercise[23].

Training Requirements:
The contractor shall provide training to the exercise team not to exceed five (5) days at the government facility.

Features:
Authorized users must have the ability to query, edit, and save their own data/scenarios and view scenario summaries. In addition, the tool must provide user and group level access control.

Field Conditions for Use:
Any authorized and authenticated user must have the ability to enter information via secure internet connection.

Users:
- DHS/IAIP/NCSD
- Cyber exercise planners to include Federal, State, Local, and Tribal governments, and critical infrastructure owners/operators

Deliverables[24]:
Development Plan; Draft Tool Architecture; Final Architecture; Prototype; Test Plan; Field Test; Effectiveness Report; Final Tool; Architecture Documentation; User Manual

Field Testing:

Key Elements to be Tested:
- The application's ease of use and security
- Realistic decision tree scenario outputs

How Many Prototypes are Required for Field Testing? One (1)

Is Participation by the Prototype Developer Desired? Yes

---

[23] *S&T Clarification: Direct support to exercise planners should be identified as a separately-costed optional task, not to exceed 1 full time equivalent (FTE) for 9 months of effort.*

[24] *S&T Clarification: Offerors should note deliverables are identified as written in a chronological fashion in terms of program execution. For this effort, the prototype should be a fully-functional tool, ready for deployment and testing in a government-sponsored test facility. After testing, an Effectiveness Report will be generated by the offeror, in conjunction with the government testing team. A final tool will be delivered as an iteration of the prototype tool, integrating changes recommended by the government testing team.*

3.1.7.3 CS3 – DHS Secure Wireless Access Prototype

Descriptive Title:
DHS Secure Wireless Access Prototype

The contractor shall propose an integration of commercial products in order to provide an end-to-end secure remote access service.

Description & Specifications

- **Performance:** Basic wireless security that relies on a combination of Service Set Identifier (SSIDs), open authentication, static Wired Equivalency Privacy (WEP) keys, Media Access Control authentication, or Wi-Fi Protected Access/Wi-Fi Protected Access 2 Pre-Shared Key (WPA/WPA2 PSK) is not sufficient for protecting Department of Homeland Security (DHS) sensitive data.

  This prototype shall demonstrate a way to connect securely to the DHS Network over the public wireless infrastructure available at many locations commonly known as "hot spots." In doing so, there should be a minimal risk involved, which must be described and the reasons for accepting that risk defined. Additionally, the prototype needs to be able to leverage the existing DHS software operating system images on notebook computers currently used to access existing major infrastructure elements.

  The prototype must be able to transmit sensitive data across these public wireless systems in a manner that sufficiently protects the data against eavesdropping via any of the commonly available packet analysis and sniffing tools. It should be noted that the goal is not to create a new secure wireless network infrastructure, but rather to use additional protection with these existing wireless networks.

  All elements in the prototype should make extensive use of fully-ratified industry standards, technologies, protocols, and signaling mechanism commonly accepted as best practices. The prototype will provide a mobile DHS user with a secure remote access service.

- **Configuration:**

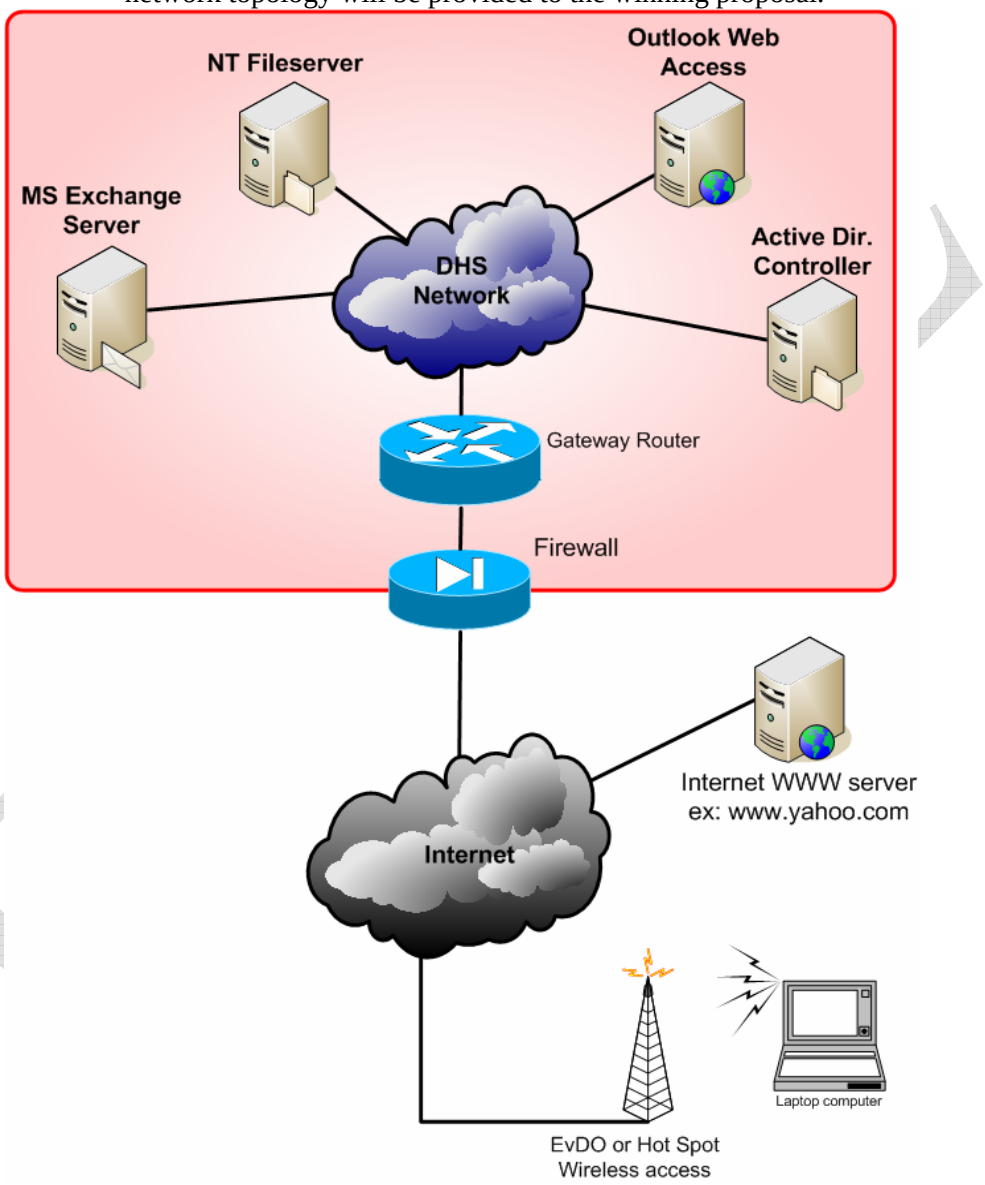
  A successful prototype will employ the following elements to ensure the performance, security, and confidentiality of sensitive information.

  - Dell notebook with wireless (802.11x) network access enabled and alternate broadband wireless technology. This computer will act as a "normal" DHS user mobile computer that will be used to connect to the DHS network via a public wireless network. This notebook computer will contain the most current DHS-certified XP configuration (image) and will also allow additional tools to be loaded to monitor the wireless data transfers. However, no administrative rights will be afforded to the end user to accomplish the overall goal of secure remote access services
  - A replica of the DHS infrastructure that contains the backend data elements, servers and systems the mobile DHS user will attempt to access securely. This includes, but is not limited to a, Microsoft Exchange server and a Microsoft Hyper Text Transfer Protocol (HTTP) server with Outlook Web Access (OWA).

FINAL

Our goal is not to test whether the HTTP server is properly configured, but rather our communications to such a server is end-to-end secure from the laptop to a point within the DHS network where it is considered mandatory to employ secure communications; this point could be either a firewall or a Virtual Private Network (VPN) concentrator or tunnel endpoint. An additional desktop computer that will monitor traffic coming into and out of this backend test bed should be included.

- See diagram below for the notional backend architecture. More details of the network topology will be provided to the winning proposal.



- **Standards:**

  Wireless standards such as Institute of Electrical and Electronics Engineers (IEEE) 802.11x wireless protocol standards, and 1xEVDO (Evolution Data Only) [and 1xRTT (Radio Transmission Technology) implicitly] could possibly be employed. Additionally, current best practices or guidance from sources such as National Institute of Standards and Technology Special Publication (NIST SP) 800-48 should be employed

- **Cost considerations:**

  - The contractor should not consider government-sponsored acceptance test team costs; those will be provided by the government.
  - Cost should not be prohibitive for deployment across DHS.

- **Training requirements:**

  The performer shall provide training to technical government personnel and members of the government-sponsored acceptance test team on the operation of the prototype prior to testing. This training is not to exceed one (1) day. Additionally, training is also required after a successful prototype has been developed. The contractor shall provide system administrators and other technical users training not to exceed one (1) day. The winning contractor will not be expected to train the end user.

- **Scenarios:**

  The following scenarios and locations are envisioned to be typical and represent the minimum level of ability to be demonstrated from the prototype. In addition, the performer should account for any infrastructure diversity in access for the locations described in the US, Canada, and Mexico:

  The locations include:

  (1) home wireless networks,
  (2) hotspots such as coffee houses,
  (3) hotel rooms, & conference centers,

  The scenarios will include:

  #1 - The user accesses basic email and file sharing services containing DHS sensitive data.

  #2 - The user accesses public websites with this laptop over the wireless infrastructure.

- **Required field conditions for use:**
  The expected operational environment of the prototype in field use is such that a mobile DHS user should be able to use a properly-configured laptop to securely connect to a DHS sensitive data source via the public wireless infrastructure (e.g. public hotspots and EvDO).

Users:

- DHS Office of the Chief Information Officer (OCIO) Wireless Management Office
- DHS S&T OCIO
- DHS employees and anyone who is authorized by DHS to access sensitive DHS data

Deliverables:

Initial Deliverables:

(1) Laptop computer used as exemplar of DHS mobile user with secure wireless access prototype
(2) Laptop computer with packet analysis and sniffing tools used in performer's internal testing of prototype.
(3) Training materials and documentation for operation of the secure wireless access prototype

FINAL

Final Deliverables:

(4) Equipment used for DHS infrastructure replica test bed
(5) Documentation describing additional tools deployed as well as configuration, parameters, and settings for the infrastructure replica test bed and the DHS mobile laptop that has wireless network access enabled and secured.
(6) Report containing empirical evidence demonstrating connections over the public wireless infrastructure (e.g. EvDO and "hot spot") that should be accepted by as sufficiently secure to carry DHS sensitive data. This report is to include data and analysis obtained from all phases of testing.

Testing:

The performer is to propose a test plan to demonstrate prototype data communication integrity and confidentiality. It is envisioned that this testing will be demonstrated by the performer, using the prototype and the DHS infrastructure replica test bed, in conjunction with the government-sponsored acceptance test team.

At a minimum, the testing should encompass the following:

- Internal testing of the prototype in a variety of conditions.
- Pre-field testing at performer's site in conjunction with government-sponsored acceptance test team.
- Field demonstration of the prototype in the locations described above (international demonstration of the prototype is not required) in conjunction with the government-sponsored acceptance test team.

Testing should demonstrate:

- Ease of use of prototype
- Data security and confidentiality
- Data Integrity

4 DELIVERABLES

The offeror may recommend a preferred format for each status report, but the Government will determine the final format. For each effort, monthly status reports will be due within one week after the last day of each month and comprehensive deliverables are due within 30 days of the conclusion of development and testing.

Monthly - Brief (not more than one page) narrative reports will be electronically submitted to the Program Manager within one week after the last day of each month. These reports will describe the previous 30 calendar days' activity, technical progress achieved against goals, difficulties encountered, recovery plans (if needed), explicit plans for the next 30-day period, and financial expenditures (including expenditures during the past 30 day period, cumulative expenditures, and projected 30 day expenditure).

FINAL

Final - For a final report, each team will provide a technical report of their work performed 40 days after the period of performance. This will include performance predictions, estimates of cost and an enumeration of remaining unknowns and uncertainties. This final report will be a cumulative, stand-alone document that describes the work of the entire development period leading up to it. It should detail how the design prototype was refined and why the refinement was undertaken. It must include any technical data gathered, such as, measurements taken, models developed, simulation results, and formulations developed. This final report should also include "lessons learned" from the effort, recommendations for future research in this area, and a comprehensive and detailed account of all funds expended.

4.1 Additional Deliverables

Performers should define additional program specific deliverables as appropriate for the proposed approach and as required by the specific topic area.

5 INFORMATION FOR OFFERORS

5.1 Eligible Applicants

This solicitation is a Broad Agency Announcement (BAA) considered to be a full and open competition. Offerors may include single entities or teams from private sector organizations, Government laboratories, Federally Funded Research and Development Centers (FFRDCs), and academic institutions. However, the Department of Energy Laboratories listed in Appendix A are excluded from submitting responses or participating as a team member under this solicitation. These laboratories are considered DHS Strategic Partner Laboratories and are prohibited because of their direct participation in DHS programs through the Office of Research and Development. All others may participate or submit a mandatory white paper and a full proposal in accordance with the requirements and procedures identified in this BAA.

Historically Black Colleges and Universities (HBCU), Minority Institutions (MI), small and disadvantaged businesses (SDB), women-owned businesses (WB), and Historically Underutilized Business Zone (HUBZone) Enterprises are encouraged to submit proposals and to join others as team members in submitting proposals; however, no portion of the BAA will be set aside for these special entities because of the impracticality of reserving discrete or severable areas of research and development under this topic.

5.2 Organizational Conflict of Interest

Organizational Conflict of Interest issues will be evaluated on a case-by-case basis as outlined in Appendix C. Offerors who have existing contract(s) to provide scientific, engineering, technical and/or administrative support directly to the program officers or other operational activities of the Science and Technology Directorate will receive particular scrutiny.

5.3 Anticipated Funding Level

HSARPA anticipates that up to **$33M** in funding will be available for award to multiple offerors under this solicitation. The Government anticipates only one award per topic, although the Government reserves the right to award none, one, or more proposals per topic. The anticipated funding level may not exceed $2M per award.

5.4 Types of Awards Including Other Transactions for Prototypes

The Government anticipates executing awards as contracts, but in exceptional circumstances awards may be executed as grants, cooperative agreements or other transactions. Section 831(a)(2) of the Homeland Security Act of 2002 (Public Law 107-296) gives the Department of Homeland Security (DHS) the same "Other Transactions for Prototypes" authority exercised by the Department of Defense (DoD) under 10 U.S.C. §2371 note. Section 831(a) (2) also imposes the same criteria for award of an "Other Transactions for Prototypes" agreement on DHS. Proposals should clearly identify which of these funding vehicles is preferred by the offeror. The Government will make the final determination as to the type of award instrument.

5.5 Registration and Submission Instructions

Offerors are required to register online, using the HSARPA BAA Website at http://www.hsarpabaa.com, prior to submitting a mandatory white paper. Instructions for registration are provided on the website. Offerors who have not registered by the mandatory white paper website registration deadline provided in Table 5.1 of Section 5.14 will not be permitted to submit a mandatory white paper and thus, will not be able to submit a proposal later. If a Government-only review is desired, offerors must indicate so during the mandatory white paper registration. If offerors fail to properly request Government-only review, then the Government shall not be liable for inadvertent release of any mandatory white paper or proposal information to non-Government reviewers. **It is very important to follow the registration instructions. Offerors must coordinate with all members of their team to ensure the registration process is done correctly and in a timely manner.**

Upon successful registration, a file will be sent to the registered e-mail address. Receipt of this file confirms your registration. **This e-mail will contain a registration number that is required for uploading both the mandatory white paper and the full proposal.** Please check the contents of the file. If they are incorrect, return to the website and make corrections. Any questions concerning the registration or mandatory white paper/proposal submission process should be directed to HSARPA by emailing BAA05-10@dhs.gov.

Following successful registration, mandatory white papers and proposals may be submitted electronically at http://www.hsarpabaa.com. **The submission of a mandatory white paper is required to be allowed to submit a full proposal. There will be no exceptions to this rule**.

5.6 Applications and Submission Information

Copies of this BAA may be downloaded from the FedBizOpps web site at www.FedBizOpps.gov or at www.hsarpabaa.com. The Government will not provide paper copies of this BAA.

5.7 Proprietary Information Protection

All data uploaded to www.hsarpabaa.com is protected from public view or download. All submissions will be considered source selection sensitive and protected accordingly.

5.8 Multiple Submissions

Organizations are permitted to submit more than one proposal or mandatory white paper to this solicitation, but each mandatory white paper/proposal can address only one topic. The Government encourages organizations to coordinate their submissions to submit one white paper

FINAL

or proposal per topic whenever possible. In the case where a single concept applies to multiple topics, offerors may submit the same mandatory white paper and proposal to each of the applicable topics addressing only one topic per mandatory white paper/proposal.

5.9 Submitting a Classified Response to this BAA

HSARPA does not anticipate that proposals submitted in response to this BAA will be classified, unless specifically addressed in the topic. Classified submittals cannot be submitted electronically at http://www.hsarpabaa.com. However, the submitter must first register online following the registration instructions provided in Section 5.5 and get a registration number. Submitters must print out the registration form and attach it as a coversheet to the classified submittal located after the classification coversheet. The classified submittal must be submitted via proper classified courier or proper classified mailing procedures as described in the National Industrial Security Program Operating Manual (NISPOM). Offerors may view this document online at http://www.dss.mil/isec/nispom.htm. Classified submittals must include ten printed proposals and one electronic copy on compact disc recordable (CD-R) media. Each copy must be accompanied by the coversheet which does not count towards the page limitation described in Section 5.11 and Section 5.12 respectively. Classified documents MUST be received by the applicable due date and time.

Classification does not eliminate the requirement for offerors to comply with all instructions and deadlines in this BAA.

For additional instructions with regards to the submission of classified proposals, contact **Angel-Santiago Pinto**, Security Officer.

Angel-Santiago Pinto, HSARPA Security Officer
angel.santiago-pinto@associates.dhs.gov
202-254-6191

5.10 Security Considerations

The Government does not anticipate the need for classified information. In the course of the program, the RTAP contractor may be required to gain access to a secured environment and data. Each contractor individual requiring access to classified information will need to be certified at the appropriate security level required for personnel, data storage, and information technology. A DD254 form will identify the security requirements.

5.11 Export Control Considerations

The Government does not anticipate that the International Traffic in Arms Regulations (ITAR) will apply to this effort. However, foreign nationals must meet the requirements for participation set by those regulations if required

5.12 Mandatory White Paper Guidance and Content

Offerors are required to register and submit mandatory white papers in advance of full proposals. Failure to submit a mandatory white paper will disqualify an offeror from submitting a full proposal. **Only one mandatory white paper per registration is allowed.**

FINAL

The lead organization must remain the same on both the mandatory white paper and the proposal. Any full proposals submitted by entities who were not the prime for the mandatory white paper submission will be considered non-responsive.

Discussion, suggestions, or advice given during communication between the Government and offerors on mandatory white paper topics is not binding. Offerors are free to submit a full proposal without regard to any feedback or advice about mandatory white papers that they may have received. Even if the feedback from the Government in response to the mandatory white paper is that a proposal based on the offered idea is unlikely to receive funding, a full proposal may still be submitted and will be evaluated uniformly with all the other proposal submissions.

Mandatory white papers should capture the essence of a proposal and are required for two purposes. First, they give the offerors an opportunity to obtain feedback from HSARPA on their planned technology development without having to go to the expense and effort of writing a complete proposal. Second, the offerors can use the provided feedback to strengthen their proposal so that negotiations can be minimized and work started rapidly. A mandatory white paper may consist of not more than seven pages including narrative, pictures, figures, tables and charts in a legible size. A one-page quad chart is required for submission with each mandatory white paper, but does not count towards the seven-page limit. Please do not include a coversheet in your electronic submission of the mandatory white paper. At the time of review, a coversheet will automatically be generated using the information you provided during the mandatory white paper registration. A coversheet is required for classified submissions. Please follow the instructions in Section 5.9 for submitting classified mandatory white papers. All properly submitted mandatory white papers that conform to the BAA requirements will be evaluated by a review panel comprised of government employees and government contractors specially selected to eliminate potential conflicts of interest. Offerors may request a government-only review, but must indicate so during the mandatory white paper registration.

Notwithstanding a request for a government-only review, the Government intends to use employees and subcontractors of a support contractor to assist in administering the evaluation of mandatory white papers and proposals. These personnel will have signed, and will be subject to, the terms and conditions of non-disclosure agreements.

After the mandatory white paper evaluation, HSARPA will promptly notify offerors to either encourage or discourage submission of a full proposal. For those white papers encouraged to submit full proposals, HSARPA will provide recommendations. Due to the large number of white papers typically submitted, HSARPA will not offer debriefings to offerors discouraged from submitting full proposals. Offerors will be given 30 days from notification to submit a full proposal. The notification letter will include recommendations and the specific deadline for submitting a full proposal.

5.12.1 Format and size limitations:
Mandatory white papers may not exceed 7 (seven) pages, and must be accompanied by a one-page quad chart. Therefore, the entire mandatory white paper submission will not exceed 8 (eight) pages. A mandatory white paper shall consist of one or more electronic files in portable document format (PDF), readable by IBM-compatible personal computers (PCs), and in a type font no smaller than 12 points. The quad chart may be submitted as a separate one-page PowerPoint-compatible file, but the rest of the mandatory white paper must be submitted in PDF format. The individual file size must be no more than 10 Megabytes (MB). Multiple 10MB files

may be used to complete the eight-page submission. **Please do not include a coversheet with your unclassified mandatory white paper. A coversheet will be automatically generated for your white paper using the information provided during registration. If a cover sheet is submitted with the unclassified mandatory white paper it will be counted toward the 7-page white paper limit.** A coversheet is required for classified submissions, and does not count toward the 7-page limit. Please follow the instructions in Section 5.9 for submitting classified mandatory white papers.

The mandatory white paper should contain the following information in the following order:

- Quad Chart (one page)
- Mandatory White Paper Body [limit of 7 (seven) pages]
  - Utility to DHS (including anticipated performance relative to goals)
  - Technical Approach
  - Capability and Summary of Personnel and Performer Qualifications and Experience
  - Cost Summary

5.12.2 Organization of Quad Chart:
For instructions and sample of a Quad Chart, please refer to Appendix E, or go to www.hsarpabaa.com.

5.12.3 Utility to DHS
Explain how the performance of your proposed solution can be expected to meet the users' requirements, specified field conditions and be measured against each of the specific technical attributes and performance requirements described in the Topic. If the prototype is successful, outline the plan to produce the device or software.

5.12.4 Technical Approach:
Describe the basic technical approach to the proposed work that demonstrates an understanding of the critical technology challenges required for achieving the goals of the topic and describe a strategy to address those issues, including a risk mitigation strategy. Address what is unique about your solution and what advantages might it afford compared to alternate approaches other performers in this field have taken. Also, address what are the key technical or engineering challenges and the timing for each that must be met in order to successfully complete this project. Describe all required material and information, which must be provided by the Government to support the proposed work.

5.12.5 Capability and Summary of Personnel and Performer Qualifications and Experience:
Address what has been the extent of your team's past experience in working with or employing the devices comprising your prototype or prototypes including the proposed facilities to accomplish the work.

5.12.6 Cost Summary:
Provide a brief summary of the cost (labor, material, consumables equipment, subcontracts, and any Government furnished equipment, resources or information (GFE, GFR, GFI). Combined direct funding and any GFE, GFR, or GFI not provided as a condition of the topic may not exceed $2M for the base effort of the mandatory white paper. **Any mandatory white paper where the base effort exceeds $2M will be considered non-responsive**.

5.13 Proposal Guidance and Content

Offerors must submit a mandatory white paper in order to submit a proposal. There will be no exceptions. Offerors do not have to register separately for proposal submission. Mandatory white paper registration and submission is sufficient to allow submission of proposals. Only one proposal per registration is allowed. The lead organization must remain the same on both the mandatory white paper and the proposal. Any full proposals submitted by entities who were not the prime for the mandatory white paper submission will be considered non-responsive.

Using the same registration number as the mandatory white paper, offerors may submit a proposal after the deadline for mandatory white paper feedback provided in Table **5.1.** Proposals must be submitted prior to the proposal submission deadline provided in Table **5.1**. Offerors can choose to alter their ideas, concepts, technical approaches, etc. or expand on their original ideas between submission of a mandatory white paper and submission of the proposal. Discussion, suggestions, or advice between the Government and offerors on mandatory white paper topics is not binding. Even if the feedback from the Government in response to the mandatory white paper is that a proposal based on the offered idea is unlikely to receive funding, a full proposal may still be submitted and will be evaluated uniformly with others. Proposals consist of two separate volumes described in detail below:

- Volume I: Technical and Management Proposal
- Volume II: Cost Proposal

The Technical and Management proposal must be submitted as one or more PDF files. The Cost Proposal may be submitted as either a PDF file or a Microsoft Excel file. Each volume must be submitted separately, and submitted to the appropriate field on the website. The maximum file size for each file is 10 MB.

5.13.1 Volume I, Technical and Management Proposal (50-page limit inclusive)

Volume I provides the primary technical description of the proposal and is the primary document to be used by reviewers. Volume I should not exceed 50 (fifty) pages, excluding the transmittal letter, in a font no smaller than 12 points. This 50-page limit includes the quad chart as well as all pictures, figures, tables, and charts in a legible size. **Proposals where Volume I exceeds the 50-page limit will be considered to be non-responsive**. Graphic images inserted into the file should minimize file size and support clear display and document printing. Nonconforming proposals may be rejected without review. The submission of other supporting materials with the proposal is strongly discouraged and if submitted, will not be reviewed.

Please do not include a coversheet with your unclassified proposal. A coversheet will be automatically generated using the information provided during the mandatory white paper registration. If a cover sheet is submitted with the unclassified proposal it will be counted toward the 50-page limit. A coversheet is required for classified submissions and does not count toward the 50-page limit. Please follow the instructions in Section 5.9 for submitting classified proposals.

5.13.1.1 Section I. Official Transmittal letter:

This is an official transmittal with authorizing official signature and Proposal Title. The letter should be scanned into the electronic proposal.

FINAL

5.13.1.2 Section II. Quad Chart:
See Appendix E.

5.13.1.3 Section III. Abstract of Proposal:
This is a one-page synopsis of the entire proposal including total costs proposed for the effort. Provide a description of the technical/engineering, and management approaches you propose to address the goals of the Topic. Highlight what is unique about your proposed solution. Include a brief summary of your concept's anticipated performance relative to the Topic goals.

This section should be separable, i.e., it should begin on a new page with the following section beginning on a new page.

5.13.1.4 Section IV. Proposal
This section describes the proposed work and the associated technical and management issues. Below are the general guidelines for writing a technical volume, but the bidder should be aware that additional details/information may be required for a particular topic.

a. **Ability of proposed work to meet the program goals.** This section is the centerpiece of the proposal and should describe the overall methodology and how it will meet the required and desired attributes and functionality specified in the BAA. Describe how the proposed prototype is suitable to the users and field environments specified. This section should also address a plan to enter production or otherwise supply the capability to DHS users if the prototype is successful.
b. **Detailed technical descriptions and approach.** Identify the critical issues and plans for execution.
c. **Statement of Work (SOW), Schedule, and Milestones.** Provide an integrated display for the proposed work, including major milestones. The section for the schedule and milestones should be separate and clearly marked. **It is important to note that the SOW will be used for the initiation of contract negotiations for selected proposals.**
d. **Deliverables.** Provide a brief summary of all deliverables proposed under this effort, including prototype hardware, technical data, computer software, or other intellectual property, test plans, and reports consistent with the objectives of the work involved and as specified in the Topic requirements.
e. **Management Plan.** Provide a brief summary of the management plan, including an explicit description of what role each participant or team member will play in the project, and their past experience in technical areas related to this proposal and complexity of project managed.
f. **Facilities.** Describe key facilities that will be used in the proposed effort. Delineate between classified and unclassified facilities.
g. **Requirements for Government Furnished Resources (GFR).** Provide a brief summary of required hardware, information, and data, which must be provided by the Government to support the proposed work, if any. Provide a detailed breakout for all GFR that is requested by the offeror.
h. **Government Data Rights**. If applicable, offerors must provide data rights structure. The Government will accept limited rights for technical data and restricted rights for computer software which the contractor has developed exclusively with private funding. However, for the technology developed and funded under this effort the Government will accept only unlimited rights, Government Purpose Rights or specially negotiated rights.

FINAL

i. **Security Plan.** Describe the rationale for what aspects of the work, if any, need to be protected, and at what level, and propose a strategy for doing so. If you propose classified work, provide the collateral clearance level held, if any, by each team member.
j. **Cost Summary.** Summarize the projected total costs for each task in each year of the effort including a summary of subcontracts, man-hours, consumables, and GFR.
k. **Similar Work**. List any other substantially similar proposals that you have currently pending with the Federal Government (proposal title, proposal number, and agency).

5.13.2 Volume II, Cost Proposal (no page limit)

There is no page limit on Volume II. Only the items outlined in this section should be included in Volume II. Additional documentation provided that is not relevant to the Cost Proposal, will not be reviewed.

5.13.2.1 Section I. Cost Response:

The cost response should be in the offeror's format. Certified cost or pricing data are not required. However, in order for the government to determine the reasonableness, realism and completeness of the Cost Proposal, the following data must be provided for each team member and in a cumulative summary:

Labor: Total labor includes direct labor and all indirect expenses associated with labor to be used in the period of performance. Labor hours shall be allocated to each work outline element and segmented by team member. A labor summary by work outline is required. Provide a breakdown of labor and rates for each category of personnel to be used on this project.

Direct Materials/Equipment: Total direct material that will be acquired and/or consumed in the period of performance. Limit this information to only major items of material and how the estimated expense was derived. For this agreement, a major item exceeds $25,000. Material costs shall be assigned to specific work outline elements.

Travel: Total proposed travel expenditures relating to the period of performance.
Limit this information to the number of trips, location, duration, and purpose of each trip.

Subcontracts: Describe major efforts to be subcontracted, the source, estimated cost and the basis for this estimate. For this award a major effort exceeds $250,000. Subcontract labor and material shall be accounted for per the Labor and Direct Materials paragraphs above. A summary chart showing each major subcontractor labor and material effort by work outline is required.

Other Costs: Any direct costs not included above. List the item, the estimated cost, and basis for the estimate. The Cost Proposal should be consistent with your proposed SOW. Activities such as demonstrations required to reduce the various technical risks should be identified in the SOW and reflected in the Cost Proposal.

Government-Furnished Equipment, Resources, and Technologies (GFE, GFR, and GFI): As stated in section 2.2 the Government may consider requests from offerors for Government-furnished equipment, resources and information. Combined direct funding and GFE, GFR, and/or GFI may not exceed $2M for the base effort of the proposal. **Any proposal where the base effort exceeds $2M will be considered non-responsive.**

FINAL

5.14 Contact Information for Questions Regarding this Solicitation

The electronic address for this correspondence related to this BAA is: **BAA05-10@dhs.gov**. To ensure proper logging and prompt response to questions about this BAA, potential submitters are encouraged to use this e-mail address for all correspondence.

The HSARPA Program Manager leading this effort is:

Mr. Maurice Swinton (HSARPA Program Manager)
hsarpa.rtap@dhs.gov

The HSARPA Contracting Officer for this effort is:

Mr. James Thompson, Contracting Officer
Homeland Security Advanced Research Projects Agency
Department of Homeland Security
Washington DC 20528
james.thompson1@dhs.gov

5.14.1 Objections to Solicitation and Award

Any objections to the terms of this solicitation or to the conduct of receipt, evaluation or award of agreements must be presented in writing within 10 calendar days of (1) the release of this solicitation or (2) the date the objector knows or should have known the basis for its objection. Objections should be provided in letter format, clearly stating that it is an objection to this solicitation or to the conduct of the evaluation or award of an agreement, and providing a clearly detailed factual statement of the basis for objection.

Failure to comply with these directions is a basis for summary dismissal of the objection. Mail objections to:

Mr. James Thompson, Contracting Officer
Homeland Security Advanced Research Projects Agency
Department of Homeland Security
Washington DC 20528
james.thompson1@dhs.gov

5.15 Solicitation and Award Schedule

To aid in the management of the anticipated large response to this solicitation, Offerors are required to register in advance before they may submit a mandatory white paper. Offerors do not need to register separately prior to proposal submission, since the same registration information will be used for the full proposal. Registration should be done at the website: http://www.hsarpabaa.com. Offerors must register by the mandatory white paper website registration deadline provided in Table 5.1.

FINAL

Date	Time	Event
28 November 2005 (Mon.)		BAA Posted (Registration Open)
20 December 2005 (Tue.)	4 PM EST	Mandatory White Paper Website Registration Deadline
3 January 2006 (Tue.)	4 PM EST	Mandatory White Paper Submission Deadline
3 February 2006 (Fri.)		Mandatory White Paper Feedback Provided (open for full proposal submission)
6 March 2006 (Mon.)	4 PM EST	Proposal Submission Deadline
6 April 2006 (Thur.)		Selections Announcement Date

Table 5.1. Schedule of Events

HSARPA plans to review all mandatory white papers in accordance with the above Solicitation and Award Schedule using the evaluation criteria described in Section 6. After the mandatory white paper review. HSARPA will notify offerors, electronically or in writing, at its discretion, either encouraging or discouraging submission of full proposals based upon this review. HSARPA does not intend to provide further feedback or a debrief to submitters of mandatory white papers for which full proposals are not encouraged.

HSARPA plans to review all proposals in accordance with the above Solicitation and Award Schedule. Proposals will be evaluated by a review panel using the criteria specified under Evaluation Criteria in Section 6. Following this review, offerors will be notified whether or not their proposal has been selected for negotiation.

Multiple awards are anticipated under this solicitation. The Government may make one or more awards per topic, but expects in most cases to make a single award per topic. The Government reserves the right to fund none, some, or all of the proposals received. It is the intention upon completion of proposal evaluation to notify offerors of an initiation of negotiation for awards or rejection of their proposal. Awards will be made based on the evaluation, funds availability, and other programmatic considerations.

6 EVALUATION CRITERIA AND SELECTION PROCESS

6.1 Mandatory White Papers

The evaluation of mandatory white papers will be accomplished through an independent technical review of each using the following criteria, which are listed in descending order of relative importance:

Criterion I: **Utility to DHS**: Potential of the prototype for meeting the required and desired topic attributes given in BAA 05-10. This evaluation factor also takes into consideration the likelihood that if the development is successful, then production capability will exist. Prototypes must work in the field environment outlined within the topic and with the specified users.

Criterion II: **Technical Approach**: Sound technical and managerial approach to the proposed work, including a demonstrated understanding of the critical technology challenges required for achieving the goals of the topic, and a strategy to address those issues, including a risk mitigation strategy and the uniqueness of the approach.

FINAL

Criterion III: **Capability**: Capability to perform proposed work and history of performance of the offeror and any team members in developing related technologies. This factor includes the skills and experience of the proposed team as well as the proposed facilities to accomplish the work.

Criterion IV: **Cost Realism**: Does the proposed cost seem reasonable and appropriate with regard to the development of the prototype?

6.2 Proposals

The evaluation of proposals will be accomplished through an independent technical review of each using the following criteria, which are listed in descending order of relative importance:

Criterion I: **Utility to DHS**: Potential of the prototype for meeting the required and desired topic attributes given in BAA 05-10. This evaluation factor also takes into consideration the likelihood that if the development is successful, then production capability will exist. Prototypes must work in the field environment outlined within the topic and with the specified users.

Criterion II: **Technical Approach**: Sound technical and managerial approach to the proposed work, including a demonstrated understanding of the critical technology challenges required for achieving the goals of the topic, and a strategy to address those issues, including a risk mitigation strategy and the uniqueness of the approach.

Criterion III: **Capability**: Capability to perform proposed work and history of performance of the offeror and any team members in developing related technologies. This factor includes the skills and experience of the proposed team as well as the proposed facilities to accomplish the work.

Criterion IV: **Cost Realism**: Does the proposed cost seem reasonable and appropriate with regard to the development of the prototype?

FINAL

7 LIST OF ATTACHMENTS

- Appendix A — List of Excluded Offerors
- Appendix B — List of Acronyms
- Appendix C — Organizational Conflict of Interest
- Appendix D — Hazardous Material Identification and Material Security Data
- Appendix E — Quad Chart Format

FINAL

Appendix A: List of Excluded Offerors

This solicitation is a Broad Agency Announcement (BAA) considered to be full and open competition. Therefore any entity other than the following Department of Energy (DoE) National Laboratories may submit responses to this solicitation:

1) Argonne National Laboratory

2) Brookhaven National Laboratory

3) Department of Energy Remote Sensing Laboratory

4) Idaho National Engineering and Environmental Laboratory

5) Lawrence Livermore National Laboratory

6) Los Alamos National Laboratory

7) Oak Ridge National Laboratory

8) Pacific Northwest National Laboratory

9) Sandia National Laboratory

10) Savannah River National Laboratory

The DoE National Laboratories listed above are excluded from submitting responses or participating as a team member under this solicitation. These laboratories are considered DHS Strategic Partner Laboratories and are prohibited because of their direct participation in DHS programs through the Office of Research and Development.

FINAL

Appendix B: List of Acronyms

2D	Two Dimensional
3D	Three Dimensional
A	Amperes
AC	Alternating Current
AMOC	Air and Marine Operations Center
AMS	Aerospace Material Specification
ANSI	American National Standards Institute
APHIS	Animal and Planet Health Inspection Service
BAA	Broad Agency Announcement
BAO	Bomb Appraisal Officer
BC	Biological Countermeasures
BTS	Border Transportation Security
C&C	Command and Control
CAP	Common Alerting Protocol
CBP	Customs and Border Protection
CBRN	Chemical Biological Radiological and Nuclear
CC	Chemical Countermeasures
CDR	Critical Design Review
CD-R	Compact Disc-Recordable
CFR	Code of Federal Regulations
COTS	Commercial Off the Shelf
CS	Cyber Security
CSI	Container Security Initiative
DC	Direct Current
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DoD	Department of Defense
DoE	Department of Energy
EC	Explosives Countermeasures
EDS	Explosives Detection System
EDXL	Emergency Data Exchange Language
EH	Electronics and Hardware
EMS	Emergency Medical Services
EOD	Explosive Ordnance Disposal
EPA	Environmental Protection Agency
ESS	Explosive Security Specialist
EST	Eastern Standard Time

FINAL

ETD	Explosives Trace Detection
EvDO	Evolution Data Only
FAMS	Federal Air Marshall Service
FAR	False Alarm Rate
FedBizOpps	Federal Business Opportunities (www.FedBizOpps.gov)
FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research and Development Centers
FGDC	Federal Geographic Data Committee
FIFRA	Federal Insecticide, Fungicide, and Rodenticide Act
FOR	Field of Regard
FOV	Field of View
FPS	Federal Protective Service
FTE	Full Time Equivalent
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFR	Government Furnished Resources
GIF	Graphic Interchange Format
GIS	Geographic Information System
GJXDM	Global Justice XML Data Model
G-OPC	USCG Office of Homeland Security Operations and Tactics
GOTS	Government Off the Shelf
HAZMAT	Hazardous Material
HAZWASTE	Hazardous Waste
HBCU	Historically Black Colleges and Universities
HEPA	High Efficiency Particulate Air
HERO	Hazards and Electronic Radiation to Ordnance
HIFLD	Homeland Infrastructure Foundation-Level Database
HSARPA	Homeland Security Advanced Research Projects Agency
HSPD	Homeland Security Presidential Directive
HTTP	Hyper Text Transfer Protocol
HUBZone	Historically Underutilized Business Zone
Hz	Hertz
IA/IP	Information Analysis/Infrastructure Protection
IBM	International Business Machines
ICE	Immigration and Customs Enforcement
ID Theft	Identification Theft
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
IMS	Ion Mobility Spectroscopy
IPR	Interim Progress Review
IR&D	Independent Research and Development

FINAL

IR/NV	Infrared/Night-Vision
IRC	Internet Relay Chat
ISO	International Organization for Standardization
ITAR	International Traffic in Arms Regulations
ITG	Information Technology – Geospatial
ITS	Information Technology – Sharing
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LE	Law Enforcement
M	Million
MAC	Month(s) after Contract
MB	Megabyte
MCUE	Modeling the Complex Urban Environment
MI	Minority Institutions
MIL-PRF	Military Standard Performance Specifications
MPH	Miles Per Hour
MS	Microsoft
MSDS(s)	Material Safety Data Sheet(s)
MSL	Mean Sea Level
MSST	Maritime Safety and Security Team
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NCSD	National Cyber Security Division
NEMA	National Electrical Manufacturers Association
NGA	National Geospatial Intelligence Agency
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NIOSH	National Institute of Occupational Safety & Health
NISPOM	National Industrial Security Program Operating Manual
NIST SP	National Institute of Standards and Technology Special Publication
O&M	Operations & Maintenance
OAG	Official Airline Guide
OASIS	Organization for the Advancement of Structured Information Standards
OCIO	Office of the Chief Information Officer
OGA	Other Government Agencies
OGC	Open GIS Consortium
OIA	Office of Information Analysis
OINT	Office of Intelligence
ORD	Office of Research & Development
OTA	Other Transaction Authority

FINAL

OWA	Outlook Web Access
PC	Personal Computer
Pd	Probability of Detection
PDF	Portable Document Format
PDR	Preliminary Design Review
POC	Point of Contact
POE	Port of Entry
PSD-WMD	Protective Security Division-Weapons of Mass Destruction
RAIC	Resident Agent in Charge
RDT&E	Research, Development, Test and Evaluation
RFIP	Rapid Field Identification of High Priority Plant Pathogens
ROSS	Resource Ordering and Status System
RTAP	Rapid Technology Application Program
RTT	Radio Transmission Technology
S&T	Science and Technology
SAIC	Special Agent in Charge
SDB	Small and Disadvantaged Businesses
SIEVE	Significant Encounters Visual Environment
SME(s)	Subject Matter Expert(s)
SOW	Statement of Work
SSI	Sensitive Security Information
SSID	Service Set Identifier
SWAT	Special Weapons and Tactics
TCL	Target Capabilities List
TECS	Treasury Enforcement Communications System
TIB	Tactical Information Branch
TIC(s)	Toxic Industrial Chemical(s)
TIFF	Tagged Image File Format
TISS	Tactical Information Sharing System
TRR	Test Readiness Review
TS/SCI	Top Secret/Sensitive Compartmented Information
TSA	Transportation Security Administration
UASI	Urban Area Security Initiative
UICDS	Unified Incident Command and Decision Support
UL	Underwriters Laboratories
US	United States
US&R	Urban Search and Rescue
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USDA	United States Department of Agriculture

FINAL

VAC	Volts Alternating Current
VDC	Volts Direct Current
VPN	Virtual Private Network
WB	Women-owned Business
WEP	Wired Equivalency Privacy
WMD	Weapons of Mass Destruction
WMF	Windows Metafile Format
WPA/WPA2 PSK	Wi-Fi Protected Access/Wi-Fi Protected Access 2 Pre-Shared Key
WTMD	Walk Through Metal Detection
WWW	World Wide Web
XML	Extensible Markup Language

FINAL

Appendix C: Organizational Conflict of Interest

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage.

(b) If any such conflict of interest is found to exist, the Contracting Officer may (I) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to mitigate or avoid such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

(1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

(2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included the mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation/Waiver. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes it can be mitigated, neutralized, or avoided, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan. If not defined, then this provision applies fully.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

FINAL

Appendix D: Hazardous Material Identification and Material Security Data (January 1997)

(a) "Hazardous material," as used in this clause, includes any material defined as hazardous under the latest version of Federal Standard No. 313 (including revisions adopted during the term of the contract).

(b) The offeror must list any hazardous material, as defined in paragraph (a) of this clause, to be delivered under this contract. The hazardous material shall be properly identified and include any applicable identification number, such as National Stock Number or Special Item Number. This information shall also be included on the Material Safety Data Sheet submitted under this contract.

Material (*If none, insert "None"*)	Identification No.
_____	_____
_____	_____
_____	_____

(c) This list must be updated during performance of the contract whenever the Contractor determines that any other material to be delivered under this contract is hazardous.

(d) The apparently successful offeror agrees to submit, for each item as required prior to award, a Material Safety Data Sheet, meeting the requirements of 29 CFR 1910.1200(g) and the latest version of Federal Standard No. 313, for all hazardous material identified in paragraph (b) of this clause. Data shall be submitted in accordance with Federal Standard No. 313, whether or not the apparently successful offeror is the actual manufacturer of these items. Failure to submit the Material Safety Data Sheet prior to award may result in the apparently successful offeror being considered non-responsible and ineligible for award.

(e) If, after award, there is a change in the composition of the item(s) or a revision to Federal Standard No. 313, which renders incomplete or inaccurate the data submitted under paragraph (d) of this clause, the Contractor shall promptly notify the Contracting Officer and resubmit the data.

(f) Neither the requirements of this clause nor any act or failure to act by the Government shall relieve the Contractor of any responsibility or liability for the safety of Government, Contractor, or subcontractor personnel or property.

(g) Nothing contained in this clause shall relieve the Contractor from complying with applicable Federal, State, and local laws, codes, ordinances, and regulations (including the obtaining of licenses and permits) in connection with hazardous material.

(h) The Government's rights in data furnished under this contract with respect to hazardous material are as follows:

FINAL

(1) To use, duplicate and disclose any data to which this clause is applicable. The purposes of this right are to—

(i) Apprise personnel of the hazards to which they may be exposed in using, handling, packaging, transporting, or disposing of hazardous materials;

(ii) Obtain medical treatment for those affected by the material; and

(iii) Have others use, duplicate, and disclose the data for the Government for these purposes.

(2) To use, duplicate, and disclose data furnished under this clause, in accordance with paragraph (h) (1) of this clause, in precedence over any other clause of this contract providing for rights in data.

(3) The Government is not precluded from using similar or identical data acquired from other sources.

(i) Except as provided in paragraph (i)(2), the Contractor shall prepare and submit a sufficient number of Material Safety Data Sheets (MSDS's), meeting the requirements of 29 CFR 1910.1200(g) and the latest version of Federal Standard No. 313, for all hazardous materials identified in paragraph (b) of this clause.

(1) For items shipped to consignees, the Contractor shall include a copy of the MSDS's with the packing list or other suitable shipping document which accompanies each shipment. Alternatively, the Contractor is permitted to transmit MSDS's to consignees in advance of receipt of shipments by consignees, if authorized in writing by the Contracting Officer.

(2) For items shipped to consignees identified by mailing address as agency depots, distribution centers or customer supply centers, the Contractor shall provide one copy of the MSDS's in or on each shipping container. If affixed to the outside of each container, the MSDS's must be placed in a weather resistant envelope.

FINAL

Appendix E: Quad Chart Format

This template will be available in Microsoft PowerPoint Format at http://www.hsarpabaa.com.

BAA Number: BAA05-10
Topic: *(Insert Topic Number)* **Offeror Name:**
Title: *(Brief/Short Title to Describe Offeror's Proposed Effort)* **Date:**

Photograph or artist's concept: Provide a simple but sufficiently detailed graphic that will convey the main idea of the final capability/use of the prototype, and its technological methodology. It should further give an idea of the size and weight of the end item.	**Operational Capability:** Provide information on how the prototype or prototype component would meet the goals listed in Section 3: 1) Performance Targets 2) Cost of Ownership 3) Prototype Characteristics
Proposed Technical Approach: Specifically, how the problem will be approached. Describe tasks to be performed. Describe any actions done to date. Describe any related on-going effort by the offeror. Describe the technology involved and how it will be used to solve the problem. Describe the key technical challenges.	**Cost and Schedule:** Provide any milestone decision points that will be required. Describe period of performance and total costs. Include the base performance period cost and length, and estimates of cost and lengths of possible option. **Deliverables:** Include all hardware, software, and data deliverables. **Corporate Information:** You must include Offeror Name, POC full name, address, phone numbers and email.